ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ имени академика С.П.КОРОЛЕВА»

В.Г. Засканов, Г. Ф. Несоленов

БЕЗОПАСНОСТЬ В СФЕРЕ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

Часть II

Самара 2005

УДК 343.37

Засканов В. Г., Несоленов Г. Ф. **Безопасность в сфере экономической деятельности:** Учеб. пособие. Ч. II/ Самар. гос. аэрокосм. ун-т, 2005. - 182 с.

ISBN 5-7883-0369-9

Даются некоторые основы знаний по информационной безопасности, необходимых для подготовки менеджеров в сфере экономической деятельности в зависимости от угрозы. Рассмотрены необходимые средства защиты по обеспечению информационной безопасности экономических систем. Затронуты отдельные вопросы электронной коммерции и защиты коммерческой тайны. Рассматриваются психологические факторы и закономерности возникновения несчастных случаев, в том числе и при чрезвычайных ситуациях, разрушающих внутреннюю среду экономических структур и влияющих на устойчивость функционирования объектов экономики.

Табл. 2. Ил. 3. Библиогр.: 45 назв.

Печатается по решению редакционно-издательского совета Самарского государственного аэрокосмического университета

Рецензенты: д-р техн. наук, проф. Гришин Г.М.,
канд. экон. наук, доц. Иванов Д.О.

ISBN 5-7883-0369-9

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ - автоматизированное рабочее место.
АС - автоматизированные системы.
АТС - автоматизированная телефонная станция.
АЭС - атомная электростанция.
БД - база данных.
БДЭ - безусловный денежный эквивалент.
БВУ - быстровозводимое убежище.
ВВ - вредные вещества.
ВНП - валовой национальный продукт.
ВТО - Всесоюзная Торговая Организация.
ГК РФ Гражданский кодекс РФ.
ГСО - глобальная среда окружения.
ИТС - информационно-телекоммуникационные системы.
КСЗ - комплекс средств защиты.
КУ - канал утечки.
ЛВЖ -легковоспламеняющиеся жидкости.
ЛПР - лицо, принимающее решение.
ЛСО - локальная среда окружения.
МТС - международные телекоммуникационные сети.
МЧС - Министерство чрезвычайных ситуаций.
НСД - несанкционированный доступ.
ОДО - ожидаемая денежная оценка.
ОВПФ - опасные и вредные производственные факторы.

ОПФ - опасный производственный фактор.

ППНН - подавители пиковых напряжений и нагрузок.

ПРД - правила разграничения доступа.

ПРУ - противорадиационное укрытие.

ПЭВМ - персональная электронно-вычислительная машина.

РПС - разрушающие программные средства.

РФ - Российская Федерация.

СБ - служба безопасности.

СВТ - средства вычислительной техники.

СДЯВ - сильнодействующие ядовитые вещества.

СКЗИ - средства криптографической защиты информации.

СНиП - строительные нормы и правила.

СОД - система ограничения доступа.

СОИ - средства обработки информации.

СОПТЖ - средняя ожидаемая продолжительность предстоящей жизни.

СУБД - система управления базами данных.

ТК - Трудовой кодекс.

ТЭС - тепловая электростанция.

ФАПСИ - Федеральное агентство правительственной связи и информации

ЦНС - центральная нервная система.

ЧП - чрезвычайные происшествия.

ЧС - чрезвычайные ситуации.

ЭВМ - электронно-вычислительная машина.

ЭД - электронный документ.

ЭМИ - электромагнитные излучения.

ЭР - экономический район.

ЭС - экономическая система.

Глава 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В соответствии с российским законодательством на Федеральное агентство правительственной связи и информации при Президенте Российской Федерации[1] (ФАПСИ) возложено обеспечение комплексной защиты информационно-телекоммуникационных систем (ИТС), технических средств, информационно-аналитических сетей и баз данных органов государственной власти России. В условиях стремительного развития информационных технологий информационная безопасность играет все большую роль в обеспечении жизненно важных интересов личности, общества и государства. Это положение подтверждается повышенным вниманием к этой проблеме большинства развитых стран мира, в которых защита национальной конфиденциальной информации стала одним из приоритетов государственной политики.

Например, во время состоявшихся в июне 1996 года слушаний в сенатском подкомитете Конгресса США было отмечено, что защита американских ИТС от информационного воздействия является одной из главных составляющих обеспечения национальной безопасности страны. С целью усиления координации проводимых работ в этом направлении бывшим директором ЦРУ Д. Дейчем было высказано предложение по созданию при Агентстве национальной безопасности США специального центра для ведения информационной войны и отражения угроз в указанной области.[2]

---

[1] Системы сертификации средств криптографической защиты.//Системы безопасности. 1995. №4. – С. 4-7.

[2] Маркоменко В. И. Защита информации в информационно-телекоммуникационных системах органов государственной власти.// Системы безопасности, связи и телекоммуникаций. 1997. № 1.

Большое внимание уделяется во всех странах и вопросам повышения ответственности за утечку конфиденциальной информации. Так, согласно законопроекту США «Об экономическом шпионаже и сохранности экономической информации» предусматривается уголовное наказание в виде лишения свободы на срок до 25 лет или штрафа до 1 млн. долл. в отношении лиц, которые путем хищения или другими незаконными способами добыли конфиденциальную коммерческую, экономическую или финансовую информацию. Этот законопроект США отражает общую мировую тенденцию к усилению контроля хранения и использования сведений закрытого характера, к ускоренному созданию необходимой правовой базы, регламентирующей методологию их комплексной защиты. Это подтверждается тем, что в настоящее время в США действует не менее шести федеральных законов, направленных на борьбу с преступностью в информационной сфере и защиту ИТС, в Великобритании – пять, в Германии – четыре.

В России также расширяется сфера законодательной базы, регулирующей принципы надежной защиты взаимоотношений личности, общества и государства в информационной сфере.

1.1 Угроза информационной безопасности в национальных информационно-телекоммуникационных системах

Проведенный Федеральным агентством РФ анализ обстановки в области обеспечения комплексной информационной безопасности в национальных информационных сетях показал реальность угроз закрытым ИТС России и необходимость безотлагательного принятия адекватных мер по обеспечению их надежной защиты.

Все чаще средства технологической агрессии как одна из форм ведения информационной войны в мирное время используются для сбора конфиденциальной информации в различных системах связи, в том числе путем несанкционированного доступа (НСД) в компьютерные сети.

Ситуация усугубляется еще и объективной невозможностью российской промышленности удовлетворить спрос на современное компьютерное оборудование. Поэтому при создании отечественных ИТС приходится использовать в основном импортные аппаратные и программно-аппаратные комплексы. Отмеченное обстоятельство существенно увеличи-

вает возможности не только иностранных спецслужб, но и лиц и организаций, заинтересованных в важной конфиденциальной информации, получать эту информацию из телекоммуникационных систем России.

ФАПСИ располагает сведениями о так называемых «скрытых функциональных возможностях» программного обеспечения и других средствах и методах перехвата информации, которые могут быть заложены в телекоммуникационные системы, и предпринимает необходимые контрмеры по их нейтрализации.

Актуальной проблемой в рассматриваемой области является решение таких наукоемких задач, как анализ программного продукта иностранного производства для выявления в нем скрытых функциональных возможностей, в том числе средств конспиративного (негласного) съема информации, реализующих деструктивные функции в системе. Эти задачи по своей трудоемкости и сложности зачастую соизмеримы с разработкой самого программного продукта и требуют значительных материальных затрат и привлечения большого количества высококлассных специалистов. Предпринимаются также попытки продвижения на российский рынок зарубежных средств защиты информации. Однако практически все такие средства разработаны с учетом интересов иностранных спецслужб. При этом иностранные правительства принимают все возможные меры по пресечению экспорта новых надежных технологий по защите информации.

Значительные проблемы возникают при вхождении отечественных информационных систем в международные информационные сети, в частности в Интернет. По данным Конгресса США, только в 1995 году «хакеры» свыше 250 тыс. раз прорывались через эту сеть в компьютеры Министерства обороны, не считая остальных важных пользователей. Наметившееся интегрирование России в международные системы телекоммуникаций и информационного обмена невозможно без комплексного решения проблем информационной безопасности. Следует постоянно помнить о защите национальных информационных ресурсов и сохранении конфиденциальности информационного обмена по мировым открытым сетям. Вполне вероятно, что на современном этапе постиндустриального развития цивилизации на этой почве может возникать политическая и экономическая конфронтация государств, новые кризисы в

международных отношениях, когда информация становится таким же стратегическим ресурсом, как нефть, газ, алмазы и пр.

Резкое обострение криминальной обстановки в стране фактически привело к необходимости переработки ранее существовавшей модели действий злоумышленников с учетом не только внешних, но уже и внутренних угроз для безопасности информации.

В последнее время в России зарегистрированы неправовые деяния:

- регулярные попытки проникновения «хакеров» в компьютерные сети органов государственной власти,
- факты утраты конфиденциальных сообщений, передаваемых средствами документальной электросвязи,
- кражи и уничтожения банковской информации и программного обеспечения систем электронных платежей,
- отправки фальшивых авизо с использованием кодов подтверждения достоверности межбанковских операций и возможностей локальных сетей коммерческих банков.

Применение для защиты конфиденциальной информации нестойких к дешифрованию средств криптографической защиты при постоянно возрастающих активности, квалификации и «вооруженности» хакеров может привести к поистине катастрофическим последствиям для экономики страны. По данным специалистов США, снятие элементов защиты информации с компьютерных систем приведет к разорению 20% средних компаний в течение нескольких часов, 48% – потерпят крах через несколько дней, 3% банков «лопнет» через несколько часов, 50% – через несколько дней.

Суммарный ежегодный ущерб от компьютерных преступлений только в странах Западной Европы составляет порядка 30 млрд. долл.

В России ущерб от компьютерных преступлений до сих пор интегрально не подсчитывался, но с учетом их возможных масштабов сумма ущерба представляется весьма значительной. В связи с этим компьютерная преступность становится важнейшей проблемой как для России, так и для всего мирового сообщества.

Перечисленные внешние и внутренние угрозы применительно к обеспечению безопасности ИТС обобщаются понятием «информационное оружие».

Защита компьютерных систем от «информационного оружия» является новым направлением в области обеспечения информационной безопасности. Эта задача стала особенно актуальной в связи с возрастающим количеством сведений о разработке зарубежными странами концепций ведения «информационной войны». Фактически «информационное оружие» в настоящее время является одной из основных угроз информационной безопасности любого государства.

1.2 Организационно-правовые методы обеспечения информационной безопасности

Складывающаяся в мире ситуация в сфере информационной безопасности требует безотлагательного принятия законодательных, организационных и технических мер на высшем государственном уровне.

Указом Президента РФ «0 мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»[3] определены меры, препятствующие распространению в России криптографических средств, не обеспечивающих надежную защиту информации. Определенный в соответствии с этим документом и другими нормативными актами порядок разработки и эксплуатации средств защиты информации позволяет надежно оградить интересы российских потребителей криптографических средств от недобросовестных производителей.

Создана инфраструктура лицензированных Федеральным агентством предприятий, организаций и фирм, активно работающих над решением задач обеспечения комплексной безопасности в ИТС.

Действуют сертификационные центры (лаборатории), которые оснащены необходимыми методическими и руководящими материалами.

Сертифицированы различные типы шифровальных средств, предназначенных для защиты как конфиденциальной информации, так и коммерческой тайны.

---

[3] Указ Президента Российской Федерации "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации". № 334 от 03.04.95.

Применение криптографических методов и средств защиты информации при современном уровне развития криптографии и электронных технологий уже сейчас стало не только более надежным, но и экономически более предпочтительным по сравнению с другими техническими и организационными мерами обеспечения безопасности.[4] Без применения средств криптографической защиты информации практически нереально надежно защитить компьютерные сети от несанкционированного доступа (НСД). В этом случае более просто решается и ряд других задач информационной безопасности в МТС. Вместе с тем в последние годы ряд коммерческих фирм и государственных промышленных предприятий вышли на рынок с предложением поставки на эксплуатацию разработанных ими средств криптографической защиты информации (СКЗИ). ФАПСИ рассмотрело эти предложения. В большинстве случаев выявлены существенные слабости в разработанных ими средствах защиты информации (например, в изделиях фирм «Блиц», «ЛАНкрипто», «Кобра Лайн», «Цикламена» и др.). Использование подобных нестойких СКЗИ недопустимо, поскольку это создает иллюзию обеспечения безопасности, порожденную заявкой производителя о высокой стойкости при отсутствии реальных гарантий надежности. Такие системы можно уподобить стальному сейфу с картонной задней стенкой.[5]

Для создания средств, способных надежно защитить конфиденциальную информацию, требуются высококвалифицированные специалисты в области криптографии, мощные измерительно-вычислительные комплексы и научно обоснованные методики их использования. Кроме того, любая сложная экономическая ситуация требует усложнения средств защиты информационных структур, т.е. при построении систем защиты телекоммуникационных систем должна проводиться единая и взвешенная экономическая и техническая политика для достижения интегральных целей государственной политики информационной безопасности. У России нет таких огромных средств, чтобы позволить себе неоправдан-

---

[4] Галатенко В.А. Информационная безопасность.//Открытые системы. 1995. № 4...6.

[5] Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.

ную роскошь создавать разнотипные телекоммуникационные системы и обеспечивать при этом должный уровень их защищенности.

По мнению ФАПСИ, несогласованная политика в области информатизации государственных и экономически значимых структур повлечет за собой в ближайшем будущем крайне негативные с точки зрения национальной безопасности страны последствия.

Во-первых, недостаточная защищенность ведомственных систем может привести к утечке или уничтожению циркулирующей в них информации.

Во-вторых, применение несовместимых информационных технологий не позволит создать единое информационное пространство, позволяющее обеспечить эффективное управление политическими и экономическими процессами в государстве.

В результате анализа степени угроз для информационного пространства России от активных злоумышленных действий по инициативе ФАПСИ и Государственной технической комиссии при Президенте РФ был предложен комплекс мер, направленных на предотвращение компьютерных преступлений.

Эти меры основаны на многолетнем опыте Федерального агентства по созданию высокозащищенных систем и их конверсионного преобразования для обеспечения безопасности конфиденциальной, не содержащей государственной тайны информации.

Разработаны рекомендации:

- по развитию специальных средств обнаружения незаконного вторжения в информационные системы,
- выработке соответствующих процедур по своевременному устранению актов вторжения,
- ускорению разработки и внедрения новейших сетевых средств защиты в интересах обеспечения конфиденциальности, целостности и аутентичности информационных услуг.

Вместе с тем работа, проводимая ФАПСИ и другими правоохранительными органами, по пресечению противоправной деятельности отдельных предприятий и фирм в области защиты информации не всегда достигает конкретных результатов. Во многом это связано с несовершенством действующего в настоящее время законодательства.

1.2.1 Руководящие документы Гостехкомиссии России

1.2.1.1 Основные положения

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации (РФ) опубликовала пять Руководящих документов, посвященных вопросам защиты от несанкционированного доступа к информации[6,7,8,9].

Идейной основой этих документов является «Концепция защиты средств вычислительной техники от несанкционированного доступа к информации», содержащая систему взглядов Гостехкомиссии на проблему информационной безопасности и основные принципы защиты компьютерных систем. С точки зрения разработчиков перечисленных документов основная задача средств безопасности – обеспечение защиты от несанкционированного доступа к информации. Если средствам контроля и обеспечения целостности еще уделяется некоторое внимание, то поддержка работоспособности систем обработки информации (как мера защиты от угроз работоспособности) вообще не упоминается.

Определенный уклон в сторону поддержания секретности объясняется тем, что эти документы были разработаны в расчете на применение в информационных системах министерства обороны и спецслужб РФ, а также недостаточно высоким уровнем информационных технологий этих систем по сравнению с современным уровнем.

---

[6] Руководящий документ Гостехкомиссии Российской Федерации "Защита от несанкционированного доступа к информации. Термины и определения". 1995.

[7] Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

[8] Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

[9] Федеральный закон "Об информации, информатизации и защите информации". № 24-ФЗ от 20.02.95.

1.2.1.2 Таксономия критериев и требований безопасности

Руководящие документы ГТК предлагают две группы критериев безопасности – показатели защищенности средств вычислительной техники (СВТ) от НСД и критерии защищенности автоматизированных систем (АС) обработки данных.[10]

Первая группа позволяет оценить степень защищенности (правда, только относительно угроз одного типа – НСД) отдельно поставляемых потребителю компонентов ВС.

Вторая группа рассчитана на полнофункциональные системы обработки данных.

1. Показатели защищенности СВТ от несанкционированного доступа устанавливаются классификацией СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под *средствами вычислительной техники* понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Эти показатели содержат требования защищенности СВТ от НСД к информации и применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры электронно-вычислительных машин (ЭВМ)). Конкретные перечни показателей определяют классы защищенности СВТ и описываются совокупностью требований. Совокупность всех средств защиты представляет комплекс средств защиты (КСЗ).

Установлено **семь** классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Показатели защищенности и установленные требования к классам приведены в табл. 1.1.

---

[10] Соколов А.В., Вихорев С.В. Как оценить угрозу безопасности информации.// Технологии и средства связи. 2000. № 5.

Таблица 1.1

Распределение показателей защищенности по классам СВТ

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчужденный физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Текстовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения: «-» – нет требований к приведенному классу; «+» – новые или дополнительные требования; «=» – требования совпадают с требованиями к СВТ предыдущего класса; КСЗ – комплекс средств защиты.

2. Требования к защищенности автоматизированных систем. Эти требования являются составной частью критериев защищенности автоматизированных систем обработки информации от НСД. Требования сгруппированы вокруг реализующих их подсистем защиты. В отличие от остальных стандартов отсутствует раздел, содержащий требования по обеспечению работоспособности системы, зато присутствует раздел, посвященный криптографическим средствам.

Другие стандарты информационной безопасности не содержат даже упоминания о криптографии, так как рассматривают ее исключительно в качестве механизма защиты, реализующего требования аутентификации, контроля целостности и т. д.

Исключением являются только «Единые критерии», однако и в них требования раздела криптографии касаются распределения ключей, все остальное регламентируется отдельными стандартами. Таксономия требований к средствам защиты АС от НСД приведена на рис. 1.1.

Рис. 1.1. Таксономия требований к средствам защиты СВТ от НСД
(Сокращения: СВТ – средства вычислительной техники; СЗИ-системы защиты информации)

1.2.1.3 Классы защищенности автоматизированных систем

Документы ГТК устанавливают **девять** классов защищенности автоматизированных систем (АС) от НСД, каждый из которых характеризуется определенной совокупностью требований к средствам защиты.

Класс защищенности средств автоматизированной техники и автоматизированных систем представляет собой определенную совокупность требований по защите средств ВТ АС от несанкционированного доступа к информации.

Классы подразделяются на **три** группы, отличающиеся спецификой обработки информации в АС. Группа автоматизированных систем определяется на основании следующих признаков:

1. Наличие в них информации различного уровня конфиденциальности.
2. Уровень полномочий пользователей ими на доступ к конфиденциальной информации.
3. Режим обработки данных в АС (коллективный или индивидуальный).

В пределах каждой группы соблюдается иерархия классов защищенности таких систем.

Класс, соответствующий высшей степени защищенности для определенной группы, обозначается индексом **№А**, где № – номер группы (от 1 до 3). Следующий класс обозначается **№Б** и т.д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – **3Б** и **3А**.

Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и (или) хранимой в этих системах на носителях различного уровня конфиденциальности. Группа содержит два класса – **2Б** и **2А**.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи этой группы имеют равные права доступа. Группа содержит **пять** классов – **1Д, 1Г, 1В, 1Б и 1А.**

В табл. 1.2 приведены требования к подсистемам защиты для каждого класса.

Таблица 1.2

Требования к классам защищенности АС

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. Идентификация. Проверка подлинности и контроль доступа субъектов в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+
к программам				+		+	+	+	+
к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов:		+		+		+	+	+	+
запуска/завершения программ и процессов (заданий, задач);				+		+	+	+	+
доступа программ к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;				+		+	+	+	+
доступа программ к терминалам, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, каталогам, файлам, записям, полям записей;				+		+	+	+	+

Окончание табл. 1.2

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
изменения полномочий субъектов доступа, создаваемых и защищаемых объектов доступа				+			+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей		+		+		+	+	+	+
2.4. Сигнализация попыток нарушения защиты									
3.Криптографическая подсистема 3.1. Шифрование конфиденциальной информации				+				+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах									+
4.Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации				+			+	+	+
4.4. Периодическое тестирование СЗИ от НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ от НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты		+		+			+	+	+

Обозначения: «+» - требование к данному классу присутствует; «СЗИ от НСД» - система защиты информации от несанкционированного доступа.

1.3 Организационно-технические методы обеспечения информационной безопасности

Информационная безопасность рассматривается как состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы. Целью информационной безопасности является целостность конфиденциальной информации за счет введения средств защиты различных уровней и разработки системы защиты информации от несанкционированного доступа.

К более надежным средствам зашиты для обеспечения информационной безопасности, как правило, относят многоуровневую защиту.

Целостность информации предполагает способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения или разрушения.

Конфиденциальной информацией считается любая информация, требующая защиты.

Многоуровневая защита – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Система защиты информации от несанкционированного доступа рассматривается как комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Федеральное агентство РФ провело комплекс работ по анализу и систематизации проблем, связанных с информационным обеспечением безопасности органов государственной власти России, экономически значимых структур, субъектов финансового и фондового рынков. Итоги проведенного анализа нашли отражение в разработанной ФАПСИ Программе создания и развития ИТКС специального назначения. Указом Президента РФ программе придан статус Президентской, а постановлением Правительства она утверждена как федеральная целевая программа.

В соответствии с Концепцией создания и развития ИТКС, информационную компоненту системы будут составлять независимые информационные ресурсы различных министерств и ведомств. При этом ИТКС не должна подменять существующие информационные системы орга-

нов государственной власти, а должна обеспечить их полноценное, эффективное использование, взаимодействие, свободный доступ к фондам (естественно, в соответствии с принятым режимом доступа к информации). Более того, ИТКС будет способна по закрытым каналам связи доводить важную информацию из независимых различных источников, расположенных в регионах России, непосредственно Президенту и Правительству Российской Федерации.

В качестве телекоммуникационной компоненты ИТКС используется созданная в настоящее время Интегрированная государственная система конфиденциальной связи России, ядром которой является высокопроизводительная защищенная сеть передачи данных с пакетной коммутацией.

Принципиальным отличием создаваемой при участии ФАПСИ ИТКС от других подобных информационных систем является обеспечение в ней надежной защиты циркулирующей информации. Разработанные в Федеральном агентстве подходы позволяют создавать для ИТКС абонентские пункты, обеспечивающие гарантированную защиту конфиденциальной информации с использованием импортной вычислительной техники.

Идеологической и методической основой работ по созданию ИТКС служит разработанная ФАПСИ «Концепция информационной безопасности ИТКС системы специального назначения, создаваемой в интересах органов государственной власти РФ».

Сформулированные в концепции основные цели, задачи и принципы обеспечения информационной безопасности в ИТКС позволяют наметить пути их решения в рамках реализации конкретных федеральных программ и выполнения соответствующих фундаментальных научных исследований и научно-технических разработок.

Система безопасности ИТКС основана на использовании в сетях и абонентских пунктах пользователей стойких криптографических средств, которые в сочетании с применяемыми организационно-режимными, программно-техническими и специальными мерами позволяют обеспечить комплексную защиту информации. При этом средства криптографической защиты строятся на основе реализации нескольких базовых криптографических алгоритмов, прошедших всесторонние исследования с

использованием последних достижений науки и техники и с участием ведущих ученых и специалистов в области шифраторостроения. Базисные ядра этих алгоритмов являются государственными криптографическими стандартами.

К **средствам криптографической защиты** относят все средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

В зависимости от конкретных условий эксплуатации базисное ядро наращивается секретными дополнительными элементами и ключевыми системами, позволяющими в случае необходимости обеспечить более высокий уровень защиты информации.

Комплекс вопросов информационной безопасности ИТКС решается криптографическими методами и средствами, реализованными в отечественных образцах шифротехники, разработка, производство и эксплуатация которых ведется по требованиям и под руководством ФАПСИ.

В концепции определены следующие первоочередные организационные мероприятия:

- Лицензирование деятельности предприятий в области защиты информации в ИТКС.
- Сертификация по требованиям безопасности ИТКС, средств защиты информации и контроля их эффективности, входящих в ИТКС технических и программных средств обработки, хранения и передачи информации по каналам связи.
- Создание и организация серийного производства сертифицированных по требованиям безопасности отечественных технических и программных средств обработки, хранения и передачи информации по каналам связи в защищенном исполнении.
- Разработка и внедрение перспективных сертифицированных средств комплексной защиты информации и методов контроля их эффективности.
- Совершенствование и стандартизация не используемых в шифросредствах специальных технических мер и средств защиты, исключающих несанкционированный доступ, перехват и дешифрование информации, передаваемой по каналам связи.

Накопленный Федеральным агентством научно-технический и кадровый потенциал позволяет России поддерживать устойчивый паритет в области защиты информации с развитыми странами мира.

О важности криптографии как одного из методов информационной защиты говорят слова, принадлежащие Дэвиду Каину, известному американскому историку криптографии: «Великая держава – это страна, которая обладает ядерными технологиями, ракетными технологиями и криптографией».

Современная криптография базируется на последних достижениях математики, ряда фундаментальных физических и инженерных дисциплин и новейших достижениях в области компьютерных технологий. Эти работы проводятся совместно с Российской Академией наук, Академией криптографии России и рядом отраслевых академий.

На основе отечественных криптографических алгоритмов и интеллектуальных возможностей отечественных ученых и инженеров можно в сжатые сроки создавать образцы шифрсредств, не уступающие лучшим зарубежным аналогам, а по ряду показателей и превосходящие их. Демонстрация последних отечественных достижений в области шифртехники на различных международных выставках выявила большой интерес к ним со стороны ведущих зарубежных фирм. Это служит подтверждением того, что России удалось в кратчайшие сроки создать продукцию, во многом соответствующую мировому уровню шифростроения, и вселяет уверенность, что и в дальнейшем отечественные шифрсредства будут пользоваться спросом на международном рынке.

Глава 2. УГРОЗА И СРЕДСТВА ЗАЩИТЫ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

2.1 Угроза безопасности и целостности информационным сетям

Рассматривая безопасность информационных систем, следует опереться на два важных понятия «угроза безопасности и целостности». Угрозы безопасности и целостности состоят в потенциально возможных воздействиях на вычислительную систему, которые прямо или косвенно могут нанести ущерб безопасности и целостности информации, обрабатываемой системой.[11,12]

Реализация угрозы называется атакой.

Человек, стремящийся реализовать угрозу, называется нарушителем правил разграничения доступа (ПРД).

Нарушитель ПРД рассматривается как субъект доступа, осуществляющий несанкционированный доступ к информации.

Любой несанкционированный доступ к информации нарушает ее конфиденциальность и приносит значительный ущерб как целостности информации, так и безопасности самих электронных систем.

Под *ущербом безопасности* принято считать нарушение состояния защищенности, содержащейся в вычислительных средствах информа-

---

[11] Карпанесян В. А. Радиоэлектронная разведка. - М., 1991.

[12] Батурин Ю. М., Жоздишевский А. М. Компьютерная преступность и безопасность. - М., 1991.

ции путем осуществления несанкционированного доступа к объектам вычислительной системы.

Ущерб целостности информации представляет собой изменение информации, приводящее к нарушению ее вида или качества.

В настоящее время существует множество классификаций видов угроз по принципам и характеру их воздействия на систему, по используемым средствам, по целям атаки и т.д.

Рассмотрим общую классификацию угроз безопасности вычислительной системе по средствам воздействия на них. С этой точки зрения все угрозы могут быть отнесены к одному из следующих классов:

- Вмешательство человека в работу вычислительных систем.
- Аппаратно-техническое вмешательство в работу вычислительных систем.
- Разрушающее воздействие на программные компоненты вычислительных систем с помощью программных средств.

Вмешательство человека в работу вычислительной системы.

К этому классу относятся организационные средства нарушения безопасности таких систем, как кража носителей информации, НСД к устройствам хранения и обработки информации, порча оборудования и т.д., и осуществление нарушителем ПРД к программным компонентам вычислительных систем (все способы несанкционированного проникновения в вычислительные системы, а также способы получения нарушителем незаконных прав доступа к их компонентам).

Меры, противостоящие таким угрозам, носят *организационный характер* (охрана, режим доступа к устройствам вычислительных систем), а также включают в себя совершенствование систем разграничения доступа и системы обнаружения попыток атак (например, попыток подбора паролей).

Аппаратно-техническое вмешательство в работу вычислительных систем. Имеется в виду нарушение безопасности и целостности информации в таких системах с помощью технических средств. Например, получение информации по электромагнитному излучению устройств вычислительных систем, электромагнитные воздействия на каналы передачи информации и другие методы.

Защита от таких угроз, кроме организационных мер, предусматривает соответствующие *аппаратные* (экранирование излучений аппаратуры, защита каналов передачи информации от прослушивания) и программные меры (шифрация сообщений в каналах связи).

Разрушающее воздействие на программные компоненты вычислительных систем с помощью программных средств. Такие средства называются *разрушающими программными средствами* (РПС).[13] К ним относятся компьютерные вирусы, «троянские кони» (или «закладки»), средства проникновения в удаленные от пользователя системы с использованием локальных и глобальных сетей. Средства борьбы с подобными атаками состоят из *программно* и *аппаратно*-реализованных систем защиты.

В последнее время происходит быстрая эволюция средств РПС от простейших программ, осуществляющих НСД, к действующим самостоятельно удаленным сетевым агентам, которые представляют собой настоящие средства информационного нападения.

Таким образом, чтобы предотвратить угрозу безопасности и целостности информации ВС от информационного нападения, необходимо применение различных способов и средств защиты информационных сетей. Но для того чтобы эти способы и средства защиты использовать, в первую очередь следует рассмотреть пути несанкционированного доступа к электронной информации. На рис. 2.1 приведена схема несанкционированного доступа к электронной информации, влияющая на безопасность ТКС.

2.2 Классификация способов и средств защиты информации

Для решения проблемы защиты информации основными средствами, используемыми для создания механизмов защиты, принято считать следующие средства защиты:[14]

- Технические.
- Программные.

---

[13] Щербаков А. Разрушающие программные воздействия. - М., 1993.

[14] Мафшик С. Механизмы защиты в сетях ЭВМ. - М., 1993.

Рис. 2.1. Пути несанкционированного доступа к информации

Технические средства. Этот вид средств реализуется в виде электрических, электромеханических, электронных устройств. Всю совокупность технических средств принято делить на аппаратные и физические устройства.

Аппаратные устройства встраиваются непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой СОД по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры).

Физические устройства реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, решетки на окнах).

Программные средства. Они представлены программами, специально предназначенными для выполнения функций, связанных с надежной защитой информации.

Регламентация. Этот вид защиты заключается в разработке и реализации в процессе функционирования СОД комплексов мероприятий, создающих такие условия автоматизированной обработки и хранения в СОД защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму. Для эффективной защиты необходимо строго регламентировать:

- структурное построение СОД (архитектура зданий, оборудование помещений, размещение аппаратуры),
- организацию и обеспечение работы всего персонала, занятого обработкой информации.

Принуждение. При таком способе пользователи и персонал СОД вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Рассмотренные способы защиты информации реализуются применением различных методов защиты, которые классифицируются:

- на организационные,
- технические,
- программные,
- законодательные,
- морально-этические.

Организационными методами защиты называются организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации СОД для обеспечения защиты информации. Эти методы защиты охватывают все структурные элементы СОД на всех этапах: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Технические методы касаются правильного подбора всех технических средств обеспечения функционирования электронно-вычислительной техники и средств защиты с целью обеспечения безопасности электронной информации.

Программные методы средств защиты позволяют обеспечить за-

щищенность информационных систем за счет вновь создаваемых программ, ограничивающих доступ к основным программным средствам ЭВМ[15] и обеспечивающих их надежную защиту от несанкционированного доступа.

К *законодательным методам* защиты относятся законодательные акты государства, которыми регламентируются правила использования и обработки информации, ограничения доступа к конфиденциальной информации и устанавливаются меры ответственности за нарушение этих правил.

К *морально-этическим методам* защиты относятся всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в определенной стране или каком-то сообществе. Эти нормы специально предназначены для выполнения функций, связанных с защитой информации.

В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого-либо одного из вышеуказанных способов защиты не обеспечивает надежного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации. В результате в дополнение к программным средствам защиты созданы следующие способы защиты информации:

- Препятствие.
- Управление доступом.
- Маскировка.
- Регламентация.
- Принуждение.

Препятствие. Этот способ физически преграждает злоумышленнику путь к защищаемой информации (на территорию и в помещения с аппаратурой, к носителям информации).

Управление доступом. Такой способ защиты информации направлен на регулирование использования всех ресурсов системы (технических, программных средств, элементов данных). Управление доступом включает следующие функции защиты:

---

[15] Расторгуев С. Программные методы защиты информации в компьютерных сетях. - М., 1993.

- идентификацию пользователей, персонала и ресурсов системы, причем под идентификацией понимается присвоение каждому названному выше субъекту или объекту персонального имени, кода, пароля и опознание субъекта или объекта по предъявленному им идентификатору,
- проверку полномочий, заключающуюся в контроле соответствия дня недели, времени суток, а также запрашиваемых ресурсов и процедур установленному регламенту,
- разрешение и создание условий работы в пределах установленного регламента,
- регистрацию обращений к защищаемым ресурсам,
- реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

Маскировка. Она относится к способу защиты информации с СОД путем ее криптографического шифрования. При передаче информации по линиям связи большой протяженности чаще всего законодательные меры не являются обязательными, однако несоблюдение их ведет обычно к потере авторитета, престижа работника или группы лиц, использующих передаваемую информацию.

Все рассмотренные виды защиты делятся на формальные и неформальные средства защиты.

Формальные средства защиты выполняют защитные функции строго по заранее предусмотренной процедуре и без непосредственного участия человека.

Неформальные средства защиты – это такие средства, которые либо определяются целенаправленной деятельностью людей, либо регламентируют эту деятельность.

2.2.1 Анализ методов защиты информации в системах обработки данных

Обеспечение надежной защиты информации предполагает следующие действия:

- Обеспечение безопасности информации представляет собой непрерывный процесс, заключающийся:
  - в систематическом контроле защищенности;
  - выявлении «узких» и «слабых» мест в системе защиты;

– обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

Безопасность электронной информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.

- Надлежащая подготовка пользователей, направленная на обучение соблюдения ими всех правил защиты.
- Сомнение в абсолютной надежности любой системы защиты. Следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

2.2.1.1 Защита информации в ПЭВМ. Каналы утечки информации

Канал утечки информации представляет собой в персональных электронно-вычислительных машинах (ПЭВМ) совокупность источника информации, материального носителя или среды распространения несущего эту информацию сигнала и средства выделения информации из сигнала или носителя.

Известны следующие виды каналов утечки:

- Электромагнитный.
- Акустический.
- Несанкционированного копирования.
- Несанкционированного доступа.

Электромагнитный канал. Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в технических средствах обработки информации. Такое поле может индуцировать токи (наводки) в близкорасположенных проводных линиях. Этот канал, в свою очередь, делится:

- на радиоканал (высокочастотные излучения),
- низкочастотный канал,
- сетевой канал (наводки на провода сети),
- канал заземления (наводки на провода заземления),
- линейный канал (наводки на линии связи между ПЭВМ).

Акустический канал. Он связан с распространением звуковых волн

в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации.

Канал несанкционированного копирования. Этот канал может быть использован при отсутствии надлежащего контроля со стороны пользователя или самостоятельного подключения хакера к ПЭВМ.

Канал несанкционированного доступа. Несанкционированный доступ к информации в ПЭВМ – действие противника, приводящее к его ознакомлению с содержанием ценной информации или пользованию программными средствами без ведома их владельца.

При несанкционированном доступе возможно заражение ПЭВМ программными вирусами.

Программные «вирусы» – программы, обладающие свойствами самодублирования, скрывающие признаки своей работы и причиняющие ущерб информации, находящейся в персональных ПЭВМ.

Компьютерные вирусы делятся на:[16]

– файловые – присоединяются к выполняемым файлам;

– загрузочные – размещаются в загрузочных секторах ПЭВМ.

Несанкционированные действия прикладных программ – действия негативного характера, не связанные с основным назначением прикладных программ.

Важным условием обеспечения несанкционированного допуска является идентификация и аутентификация. Их можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов.

Идентификация и аутентификация – это первая линия обороны, «проходная» информационного пространства организации.

Аутентификация заключается в проверке принадлежности субъекту доступа предъявленного им идентификатора или подтверждение подлинности.

Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова «аутентификация» иногда используют сочетание «проверка подлинности». Субъект может подтвердить свою подлинность, если предъявит, по крайней мере, одну из следующих сущностей:

---

[16] Пилюгин П. Компьютерные вирусы: Курс лекций. - М., 1991.

- нечто, что он знает: пароль, личный идентификационный номер, криптографический ключ и т.п.,
- нечто, чем он владеет: личную карточку или иное устройство аналогичного назначения,
- нечто, что является частью его самого: голос, отпечатки пальцев и т.п. (т. е. свои биометрические характеристики),
- нечто, ассоциированное с ним, например, координаты.

Идентификатор доступа представляет собой уникальный признак субъекта или объекта доступа.

Идентификация состоит в присвоении субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификация позволяет субъекту–пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя.

Надежная идентификация и аутентификация затруднена по ряду принципиальных причин.

Во-первых, компьютерная система основывается на информации в том виде, в каком она была получена; строго говоря, источник информации остается неизвестным. Например, злоумышленник мог воспроизвести ранее перехваченные данные. Следовательно, необходимо принять меры для безопасного ввода и передачи идентификационной и аутентификационной информации; в сетевой среде это сопряжено с особыми трудностями.

Во-вторых, почти все аутентификационные сущности можно узнать, украсть или подделать.

В-третьих, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора, с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это повышает вероятность подглядывания за вводом.

В-четвертых, чем надежнее средство защиты, тем оно дороже.

Необходимо искать компромисс между надежностью, доступностью, стоимостью, удобством использования и администрирования средств идентификации и аутентификации. Обычно компромисс достигается за

счет комбинирования двух первых из перечисленных базовых механизмов проверки подлинности.

Наиболее распространенным средством аутентификации являются пароли.

Пароль – это идентификатор субъекта доступа, который является его (субъекта) секретом.[17]

Система сравнивает введенный и ранее заданный для определенного пользователя пароль. В случае совпадения подлинность пользователя считается доказанной.

Главное достоинство парольной аутентификации заключается в простоте и привычности. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Надежность паролей основывается на способности помнить их и хранить в тайне. Ввод пароля можно подсмотреть. Пароль можно угадать методом грубой силы, используя, быть может, словарь. Если файл паролей зашифрован, но доступен на чтение, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор.

Пароли уязвимы по отношению к электронному перехвату – это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход – использовать криптографии для шифрования паролей перед передачей по линиям связи или вообще их не передавать, т.к. это делается в сервере аутентификации Kerberos.

Тем не менее значительно повысить надежность парольной защиты позволяют следующие меры:

– наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);

---

[17] Руководящий документ "Защита от несанкционированного доступа к информации. Термины и определения". Государственная техническая комиссия при президенте Российской Федерации.

– управление сроком действия паролей, их периодическая смена;

– ограничение:

- доступа к файлу паролей,
- числа неудачных попыток входа в систему, что затруднит применение метода грубой силы;

– обучение и воспитание пользователей;

– использование программных генераторов паролей, которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.

К другим средствам, постепенно набирающим популярность и обеспечивающим наибольшую эффективность по защищенности информации, можно отнести секретные *криптографические ключи пользователей* – средства криптографической защиты информации.

Средства криптографической защиты информации – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации, основанные, например, на применении токенов.

Токен – это предмет или устройство, владение которым подтверждает подлинность пользователя.

Различают токены с памятью (пассивные, которые только хранят, но не обрабатывают информацию) и интеллектуальные токены (активные). Самой распространенной разновидностью токенов с памятью являются карточки с магнитной полосой. Для использования таких токенов необходимо устройство чтения, снабженное также клавиатурой и процессором. Обычно пользователь набирает на этой клавиатуре свой личный идентификационный номер, после чего процессор проверяет его совпадение с тем, что записано на карточке, а также подлинность самой карточки. Таким образом, здесь фактически применяется комбинация двух способов защиты, что существенно затрудняет действия злоумышленника.

В последнее время набирает популярность аутентификация путем выяснения координат пользователя. Идея состоит в том, чтобы пользователь посылал координаты спутников системы GPS (Global Positioning

System), находящихся в зоне прямой видимости. Сервер аутентификации знает орбиты всех спутников, поэтому может с точностью до метра определить положение пользователя.

Аппаратура GPS сравнительно недорога и апробирована, поэтому в тех случаях, когда легальный пользователь должен находиться в определенном месте, указанный метод проверки подлинности представляется весьма привлекательным.

Очень важной и трудной задачей является администрирование службы идентификации и аутентификации. Необходимо постоянно поддерживать конфиденциальность, целостность и доступность соответствующей информации, что особенно непросто в разнородной сетевой среде. Целесообразно, наряду с автоматизацией, применить максимально возможную централизацию информации. Достичь этого можно, применяя выделенные серверы проверки подлинности (такие как Kerberos) или средства централизованного администрирования (например, CA-Unicenter).

Некоторые операционные системы предлагают сетевые сервисы, которые могут служить основой централизации административных данных.

Централизация облегчает работу не только системным администраторам, но и пользователям, поскольку позволяет реализовать важную концепцию единого входа. Единожды пройдя проверку подлинности, пользователь получает доступ ко всем ресурсам сети в пределах своих полномочий.

2.2.1.2 Управление доступом

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты – пользователи и процессы могут выполнять над объектами – информацией и другими компьютерными ресурсами. Речь идет о логическом управлении доступом, который реализуется программными средствами. К таким средствам можно отнести:

- Логическое управление доступом.
- Контроль прав доступа.
- Идентификатор субъекта.
- Атрибуты субъекта.
- Место действия.
- Время действия.

- Внутренние ограничения сервиса.
- Ограничивающий интерфейс.
- Криптография.
- Экранирование.

Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей. Задача логического управления доступом состоит в том, чтобы для каждой пары (субъект, объект) определить множество допустимых операций, зависящее от некоторых дополнительных условий, и контролировать выполнение установленного порядка.

Контроль прав доступа производится разными компонентами программной среды – ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением (таким как монитор транзакций) и т.д.

При принятии решения о предоставлении доступа обычно анализируется следующая информация.

Идентификатор субъекта (идентификатор пользователя, сетевой адрес (компьютера и т.п.). Подобные идентификаторы являются основой добровольного управления доступом.

Атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности - основа принудительного управления доступом.

Место действия (системная консоль, надежный узел сети и т. п.).

Время действия (большинство действий целесообразно разрешать только в рабочее время).

Внутренние ограничения сервиса (число пользователей согласно лицензии на программный продукт и т.п.).

Удобной надстройкой над средствами логического управления доступом является *ограничивающий интерфейс,* когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ.

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во

многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них и, в то же время, последним защитным рубежом.[18,19]

Различают два основных метода шифрования, называемые *симметричными* и *асимметричными*.

В первом – *симметричном* методе шифрования один и тот же ключ используется и для шифровки, и для расшифровки сообщений. Существуют весьма эффективные методы симметричного шифрования. Имеется и стандарт на подобные методы.[20]

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это ставит новую проблему рассылки ключей. С другой стороны, получатель, имеющий шифрованное и расшифрованное сообщение, не может доказать, что он получил его от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать и сам.

В ***асимметричных*** методах применяются два ключа. Один из них, несекретный, используется для шифровки и может публиковаться вместе с адресом пользователя, другой - секретный, применяется для расшифровки и известен только получателю. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (100-значными) простыми числами и их произведениями.

Асимметричные методы шифрования позволяют реализовать так называемую электронную подпись, или электронное заверение сообщения. Идея состоит в том, что отправитель посылает два экземпляра сообщения – открытое и дешифрованное его секретным ключом (естественно, дешифровка незашифрованного сообщения на самом деле есть форма шифрования). Получатель может зашифровать с помощью открытого ключа отправителя дешифрованный экземпляр и сравнить с открытым экземпляром. Если они совпадут, личность и подпись отправителя можно считать установленными.

---

[18] Гроувер Д. Защита программного обеспечения. - М., 1992.

[19] Ловцов Д. Контроль и защита информации в АСУ. - М., 1992.

[20] ГОСТ 28147-89. Система обработки информации. Зашита криптографическая. Алгоритмы криптографического преобразования.

Существенным недостатком асимметричных методов является их низкое быстродействие. Вот почему их приходится сочетать с симметричными методами, при этом следует учитывать, что асимметричные методы на 3-4 порядка медленнее симметричных. Так, для решения задачи рассылки ключей сообщение сначала симметрично шифруют случайным ключом, затем этот ключ шифруют открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Экранирование. Экран – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран выполняет свои функции, контролируя все информационные потоки между двумя множествами систем.

В простейшем случае экран состоит из двух механизмов, один из которых ограничивает перемещение данных, а второй, наоборот, ему способствует. В общем случае экран или полупроницаемую оболочку удобно представлять себе как последовательность фильтров. Каждый из них может задержать данные, а может и сразу «перебросить» их «на другую сторону». Кроме того, допускаются передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Помимо функций разграничения доступа экраны осуществляют также протоколирование информационных обменов.

Важным понятием экранирования является *зона риска,* определяемая как множество систем, которые становятся доступными злоумышленнику после преодоления экрана или какого-либо из его компонентов.

Для повышения надежности защиты экран реализуют как совокупность элементов, так что «взлом» одного из них еще не открывает доступ ко всей внутренней сети.

Экранирование и с точки зрения сочетания с другими сервисами безопасности, и с точки зрения внутренней организации использует идею многоуровневой защиты.

Многоуровневая защита – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

За счет этого внутренняя сеть оказывается в пределах зоны риска только в случае преодоления злоумышленником нескольких по-разному

организованных защитных рубежей. Экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями.

Небольшими сетями пользуются в основном небольшие организации, где все сотрудники знают друг друга и доверяют друг другу. Однако даже в этом случае сеть должна обеспечивать хотя бы минимальные средства защиты информации своих пользователей.

В любой организации найдутся документы и сведения, которые не обязательно знать всем пользователям местной сети. Такая информация должна храниться в специальном каталоге, доступ к которому имеют только уполномоченные лица. Чаще любопытство, чем злой умысел сотрудников заставляет их прочитывать чужие файлы.

Далеко не каждый пользователь сети настолько силен и в других компьютерных системах, чтобы иметь неограниченный доступ к сетевым дискам. Одна неосторожная команда может уничтожить весь каталог сетевых файлов. Одна из причин, по которой в сетях устанавливают систему защиты, состоит в том, чтобы уберечь сетевую информацию от необдуманных действий пользователей.

Первый шаг по установке системы защиты состоит в создании специальных *пользовательских входов,* предоставляющих доступ к сети только определенному составу пользователей. Если пользователь не имеет своего входа, он не сможет войти в сеть.

Каждый вход связан с идентификатором пользователя, который вводится при входе в сеть.

Кроме пользовательского кода, вход содержит также другую информацию о своем владельце: пароль, полное имя и *права доступа,* которые определяют, какие действия и сетевые команды позволено использовать в работе этому сотруднику, а какие нет.

Иногда система установлена таким образом, что некоторая группа пользователей может работать в сети только в определенный период времени.

В некоторых системах существует возможность открывать специализированные входы.

Возможность создания специализированных входов значительно облегчает работу, так как можно предоставить равные права пользования

сетью некоторой группе сотрудников. Однако дело в том, что пользователи специализированного входа работают с одним и тем же паролем. Это значительно ослабляет систему защиты сети, поскольку она действует эффективнее, если каждый пользователь имеет свой личный пароль и хранит его в строжайшем секрете.

Если есть необходимость предоставить одинаковые права доступа некоторой группе сотрудников, лучше пользоваться неспециализированными, *групповыми входами*. В этом случае каждый пользователь входа имеет как бы отдельный подвход с собственным идентификатором и паролем, однако всем абонентам группового входа предоставляются равные права при работе с сетевой системой. Такой подход намного надежнее, поскольку каждый сотрудник имеет свой личный сетевой пароль.

Одним из важнейших аспектов системы сетевой защиты является система личных паролей сотрудников.

Иногда устанавливают также время действия пароля. Например, 30 дней. По истечении этого срока пользователь должен сменить пароль. Это не слишком удобно, однако сокращает риск того, что кто-либо узнает пароль и захочет им воспользоваться немного позже.

Пользовательские входы и пароли – это первая линия обороны системы защиты.

После того как пользователь получил доступ к сети, введя правильный идентификатор и пароль, он переходит ко второй линии, предлагаемой системой защиты: сеть определяет привилегии, которые имеет пользователь.

Все пользователи сети были задуманы как равные сотрудники одной системы. Но некоторые из них имеют определенные дополнительные права. Привилегии отличают таких пользователей от остальных сотрудников.

От типа сетевой операционной системы зависит, какие именно привилегии можно устанавливать в своей сети.

Обычно права доступа распространяются на целые каталоги, хотя возможно установить и специальный доступ к некоторым отдельным файлам или группам файлов. При этом используется специализированное имя файла.

В большинстве сетей права доступа устанавливаются на весь каталог

целиком и распространяются на все подкаталоги, если только на какие-нибудь из них не наложены специальные права.

Главным отличием атрибутов DOS от прав доступа в сетевых системах является то, что значение атрибута распространяется на всех пользователей, желающих работать с файлом. В то же время права доступа у пользователей разные; тогда как один из них имеет право только читать файл, другой может пользоваться неограниченным доступом к этой информации.

Понятно, что как минимум один человек в сети должен иметь неограниченный доступ ко всей информации, хранящейся в сети, и ко всем сетевым ресурсам. Такой человек называется *контролером сети,* или *администратором.* Он несет ответственность за установку и работу системы защиты. Вот почему на этого пользователя не налагаются никакие защитные ограничения.

2.2.1.3 Управленческие меры обеспечения информационной безопасности

Главная цель мер, предпринимаемых на управленческом уровне, – сформировать Программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Основой программы является *многоуровневая политика безопасности,* отражающая подход коммерческого учреждения к защите своих информационных активов.

Многоуровневая политика безопасности предполагает управление доступом к электронной информации на основе многоуровневой защиты.

Мандатное управление доступом рассматривается как разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Дискретное управление доступом предполагает разграничение доступа между поименованными субъектами и поименованными объектами.

Субъект с определенным правом доступа может передать это право любому другому субъекту.

Метка конфиденциальности (**метка**) представляет собой элемент

информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Многоуровневая защита определяет защиту, обеспечивающую разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Внедрение многоуровневой защиты возможно только на основании разработки модели нарушителя правил разграничения доступом.

Модель нарушителя правил разграничения доступа рассматривается в виде абстрактного (формализованного или неформализованного) описания нарушителя правил разграничения доступа.

Нарушителем правил разграничения доступа рассматривается субъект доступа, осуществляющий несанкционированный доступ к информации.

Все рассмотренные меры дают возможность обеспечить управление доступом к электронным средствам информации.

Глава 3. БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ

3.1 Корпоративные сети и их безопасность

Перед тем как приступить к созданию системы защиты, в первую очередь следует определить, от чего надо защититься.

От того, насколько правильно будут оценены возникающие угрозы безопасности информации, во многом зависит и выбор оптимального режима защиты. Оптимальный режим защиты зависит от значимости информации, которую необходимо защищать от посторонних лиц, и определенных затрат по созданию системы ее защиты. И чем ценнее информация, тем больше средств необходимо для ее защиты. Поэтому применение средств защиты предопределяет выбор оптимального соотношения методов защиты, максимально учитывающих уже имеющиеся разработки, и стоимости этих средств защиты.

Жизнь современной фирмы невозможно представить без хорошо развитой корпоративной сети, обеспечивающей постоянный обмен деловой информацией независимо от местонахождения пользователей. Обеспечение безопасности деятельности (в широком смысле) любой фирмы, в том числе и коммерческой, реализуется созданием системы защиты.

Система защиты предполагает наличие продуманного комплекса мер и средств, направленных на выявление, парирование и ликвидацию различных видов угроз. При этом надо помнить, что одни и те же методы могут быть использованы для парирования различных угроз. Например, железобетонный бункер защищает не только людей от превратностей судьбы, но и обеспечивает в какой-то степени целостность информационных процессов.

Система защиты должна разрабатываться от различного вида угроз и условий значимости информации в соответствии с требованиями федеральных законов и Руководящих документов, определяющих условия надежной защищенности корпоративных сетей в том числе.

Система защиты информации от НСД представляет собой комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Средство криптографической защиты информации рассматривается в виде средства вычислительной техники, осуществляющего криптографическое преобразование информации для обеспечения ее безопасности.

Система защиты секретной информации представлена комплексом организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

Актуальность решения проблемы защиты информации заключается:

– в невозможности:

- искажения информации, необходимой для принятия ответственных бизнес-решений,
- нанесения непоправимого урона деловой репутации фирмы,
- принятия ошибочных решений, приводящих к значительному материальному ущербу;

– в блокировании процесса ее получения от партнеров или сотрудников;

– во внедрении в оборот ложной информации;

– в разрушении имеющихся информационных ресурсов, содержащих финансовую, маркетинговую или технологическую информацию.

Информация, обрабатываемая в корпоративных сетях, особенно уязвима из-за существенного повышения возможности несанкционированного использования, отсутствия своевременной модификации информации, введения в оборот ложной информации.

Введению в оборот ложной информации в настоящее время способствуют:

- Увеличение:

– объемов обрабатываемой, передаваемой и хранимой в компьютерах информации;

– числа удаленных рабочих мест.

- Сосредоточение в базе данных информации различного уровня важности и конфиденциальности.
- Расширение доступа круга пользователей к информации, хранящейся в базе данных, и к ресурсам вычислительной сети.
- Широкое использование для связи пользователей глобальной сети Internet и различных каналов связи.
- Автоматизация обмена информацией между компьютерами пользователей.

Все это говорит о большой уязвимости корпоративных сетей. Чтобы решить проблему их защищенности, следует рассмотреть, что в этих сетях защищать и как защищать.

3.1.1 Модель корпоративной сети

Основное назначение любой корпоративной сети состоит в обязанности доставлять необходимую информацию пользователю, вне зависимости от его местонахождения в минимально короткий срок. Система защиты должна не мешать, а наоборот, способствовать выполнению основной функции – своевременному обмену деловой информации в полном объеме. К тому же система защиты не должна снижать скорость получения информации и обмена информацией.

В связи с этим следует учитывать, что некорпоративная сеть делается под систему защиты, а эта защита помогает корпоративной сети и является вспомогательной (но очень важной!) системой. Из этого постулата следует, что прежде чем переходить к построению модели системы защиты, необходимо определиться с моделью самой корпоративной сети, принимая во внимание, что двух повторяющихся сетей нет.

Модель защиты рассматривается в виде абстрактного (формализованного или неформализованного) описания комплекса программно-технических средств и (или) организационных мер защиты от НСД.

Каждая корпоративная сеть уникальна по-своему, но можно выделить основные элементы, присущие любой корпоративной сети и построить достаточно упрощенную, но адекватную модель такой сети с учетом того, что она была бы способна выполнять все основные функции и содержала бы весь набор необходимых для функционирования элементов. На рис. 3.1 представлена в общем виде корпоративная сеть, удовлетворяющая описанным требованиям.

Из анализа такой модели следует, что основным объектом изучения является информация, обрабатываемая в корпоративной сети. Информация же обрабатывается с помощью специального инструмента – программного обеспечения. Поэтому базисом любой корпоративной сети является общесистемное программное обеспечение. Это обеспечение может содержать различные окружающие среды, программные оболочки, программы общего назначения, текстовые процессоры, редакторы и интегрированные пакеты программ, системы управления базой данных.

Кроме того, для обработки информации используется также прикладное программное обеспечение, т. е. такие программы, которые разрабатываются специально для решения специализированных задач фирмы и в ее интересах.

В процессе обработки информации используются различные технические устройства обработки, хранения и передачи данных.

Информация может поступать с автоматизированного рабочего места (АРМ) по внутренним и внешним каналам связи, при этом информация может вводиться как с клавиатуры, так и с внешних носителей информации. Кроме того, сеть может использовать информационные ресурсы других учреждений и организаций и ресурсы глобальных телекоммуникационных сетей.

Под понятием «*пользователь корпоративной сети*» понимаются зарегистрированные в установленном порядке персоны (организации), наделенные определенными полномочиями доступа в электронной сети.[21]

В рамках своих полномочий пользователь может осуществлять толь-

[21] Подшибихин Л. И. Особенности правовой охраны программ для ЭВМ и баз данных в Российской Федерации.// Вопросы защиты информации, 1994.

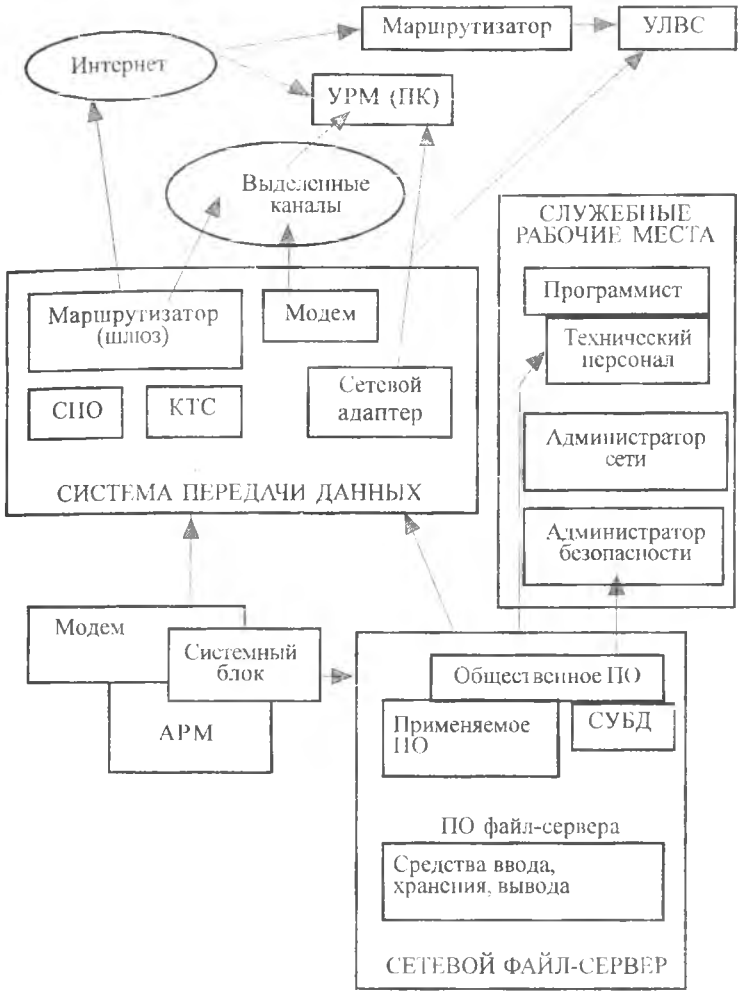

Рис. 3.1. Обобщенная модель корпоративной сети: УЛВС - удаленная локальная вычислительная сеть; УРМ – удаленное рабочее место (персональный компьютер); КТС – канальные технические средства; СПО – специальное программное обеспечение; АРМ – автоматизированное рабочее место

ко разрешенные ему действия с использованием общесистемного и прикладного программного обеспечения.

Обработка информации в сети осуществляется под контролем администраторов системы, а ее защиты – администраторов безопасности, которые выполняют свои функции, имея специализированные рабочие места. Эти места не всегда позволяют получить доступ к обрабатываемой информации, но всегда позволяют повлиять на процесс ее обработки, а также модернизацию инструмента обработки.

Администратор защиты является субъектом доступа, ответственным за защиту АС от НСД к электронной информации.

Для разработки прикладного программного обеспечения, адаптации общесистемного программного обеспечения и поддержания сети в работоспособном состоянии, как правило, привлекаются специалисты-программисты и технический персонал, которые так же имеют ограниченные возможности по доступу к самой информации, но неограниченные возможности по изменению программного обеспечения и процессов обработки информации.

Корпоративную сеть можно представить в виде системы, состоящей из ряда аппаратно-программных подсистем: рабочего места руководителя, УРМ, рабочего места администратора безопасности и системы, защитного средства вычислительной техники и системы разграничения доступа.

Защитное средство вычислительной техники (защищенная АС) рассматривается как средство вычислительной техники и (или) АС, в котором реализован комплекс средств защиты.

Система разграничения доступа представляет собой совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или АС.

Каждая из этих аппаратно-программных подсистем является относительно самостоятельной системой.

Такой подсистеме присущи признаки общей системы. Поэтому с точки зрения защиты информации здесь применим принцип декомпозиции. Согласно этому принципу механизм воздействия угроз безопасности информации применим как к системе в целом, так и к отдельной подсистеме. Это важное условие, которое позволяет правильно оценить воз-

действие угроз безопасности информации на отдельные элементы корпоративной системы, особенно на ее автономные элементы.

В настоящее время для защиты информации разработано множество различных вариантов моделей угрозы безопасности информации. Это объясняется стремлением специалистов более точно описать многообразные ситуации воздействия на информацию и определить наиболее адекватные меры парирования.

В принципе, можно пользоваться любой моделью, необходимо только убедиться, что она описывает максимально большое число факторов, влияющих на безопасность информации. Кроме того, выбирая модель защиты информации, следует, прежде всего, исходить из того, что для пользователя, т. е. потребителя информации и информационных услуг, оказываемых корпоративной сетью, не важно, какие причины нарушили информационную структуру корпоративной сети. Для пользователя важно, что во всех случаях независимо от причины итог для него одинаков – понесенные убытки (моральные или материальные).

Угроза безопасности информации – это действие, направленное против объекта защиты, проявляющееся в опасности искажений и потерь информации. Надо оговориться, что речь идет не обо всей информации, а только о той ее части, которая, по мнению ее собственника (пользователя), имеет коммерческую ценность (информация как товар) или подлежит защите в силу закона (конфиденциальная информация).

Необходимо также учитывать, что источники угроз безопасности могут находиться как внутри фирмы – внутренние источники, так и вне ее – внешние источники.

Такое деление оправдано потому, что для одной и той же угрозы (например, кража) методы парирования для внешних и внутренних источников будут разными.

При защите корпоративных сетей используются различные широко применяемые в настоящее время варианты моделей угроз, разработанные специалистами в области защиты информации государственных и негосударственных научных учреждений.

Исходя из проведенного анализа модели корпоративной сети, все

источники угроз безопасности информации, циркулирующей в этой сети можно разделить на три основные группы угроз, обусловленных:

- действиями субъекта (антропогенные угрозы),
- техническими средствами (техногенные угрозы),
- стихийными источниками.

Первая группа наиболее обширна и представляет наибольший интерес с точки зрения организации парирования этих угроз, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия этим угрозам управляемы и напрямую зависят от воли организаторов защиты информации.

Субъекты, действия которых могут привести к нарушению безопасности информации, могут быть, как внешние, так и внутренние.

К *внешним* субъектам, угрожающим информационной безопасности можно отнести:

- криминальные структуры,
- рецидивистов и потенциальных преступников,
- недобросовестных партнеров,
- конкурентов,
- политических противников.

Внутренние субъекты угрозы информации следующие:

- персонал:
- учреждения,
- филиалов,
- лица с нарушенной психикой,
- специально внедренные агенты.

Основываясь на результатах международного и российского опыта, действия субъектов могут привести к ряду нежелательных последствий, среди которых применительно к корпоративной сети можно выделить такие виды угроз, как:

- Кража:

– технических средств (винчестеров, ноутбуков, системных блоков);

– носителей информации (бумажных, магнитных, оптических и пр.);

– информации (чтение и несанкционированное копирование);

– средств доступа (ключи, пароли, ключевая документация и т. п.).

- Подмена (модификация):

– операционных систем;

– систем управления базами данных (СУБД);

– прикладных программ;

– информации (данных, отрицание факта отправки сообщений);

– паролей и правил доступа.

- Уничтожение (разрушение):

– технических средств (винчестеров, ноутбуков, системных блоков);

– носителей информации (бумажных, магнитных, оптических и др.);

– программного обеспечения (операционных систем, СУБД, прикладного программного обеспечения);

– информации (файлов, данных);

– паролей и ключевой информации.

- Нарушение нормальной работы (прерывание):

– скорости обработки информации;

– пропускной способности каналов связи;

– объемов:

- свободной оперативной памяти,
- свободного дискового пространства,
- электропитания технических средств.

- Ошибки:

– при инсталляции программного обеспечения, операционных систем, СУБД;

– написании прикладного программного обеспечения;

– эксплуатации:

- программного обеспечения,
- технических средств.

- Перехват информации (несанкционированный) за счет:

- полей электромагнитных излучений (ЭМИ) от технических средств;
- наводок:

- по линиям электропитания,

- посторонним проводникам,
- акустическому каналу;

• средств вывода при:
- обсуждении вопросов,
- подключении к каналам передачи информации;

• нарушения установленных правил доступа (взлом).

Вторая группа содержит угрозы менее прогнозируемые, напрямую зависящие от свойств техники и поэтому требующие особого внимания.

Технические средства, содержащие потенциальные угрозы безопасности информации, так же могут быть внутренними и внешними.

Внутренние технические средства – это:

• некачественные:
- технические средства обработки информации,
- программные средства обработки информации;

• вспомогательные средства (охраны, сигнализации, телефонии);

• всевозможные другие технические средства, применяемые в учреждении.

К *внешним* средствам относят:
– средства связи,[22,23]
– близко расположенные опасные производства,
– сети инженерных коммуникаций (энерго-, водоснабжения, канализации),
– транспорт.

Последствиями применения таких технических средств, напрямую влияющих на безопасность информации, могут быть:

• Нарушение нормальной работы:
• из-за несоблюдения установленных правил доступа;
• сбоя и изменения работоспособности:
- системы обработки информации,
- связи и телекоммуникаций;
• старения носителей информации и средств ее обработки;

---

[22] Ярочкин В. И. Подслушивание телефонных переговоров и меры борьбы с подслушиванием: Учеб. пособие. - М., 1993.

[23] Долуханов М. А. Оптимальные методы передачи сигналов по линиям радиосвязи. - М., 1965.

- разрушения;
- воздействия электромагнитных излучений (ЭМИ) и полей на технические средства.

- Уничтожение (разрушение):
  - программного обеспечения, операционных систем, СУБД;
  - средств обработки информации (СОИ) (броски напряжений, протечки);
  - помещений;
  - информации (размагничивание, радиация, протечки и пр.);
  - персонала.
- Модификация (изменение):
  - программного обеспечения, операционных систем, СУБД;
  - информации при передаче по каналам связи и телекоммуникациям.

Третью группу составляют угрозы, которые совершенно не поддаются прогнозированию и поэтому меры их парирования должны применяться всегда. В эту группу входят стихийные источники, составляющие потенциальные угрозы информационной безопасности. Они, как правило, являются внешними по отношению к рассматриваемому объекту и под ними понимаются, прежде всего, природные катаклизмы:

- пожары,
- землетрясения,
- наводнения,
- ураганы,
- другие форс-мажорные обстоятельства,
- непредвиденные различные обстоятельства,
- необъяснимые явления.

Эти природные и необъяснимые явления также влияют на информационную безопасность, опасны для всех элементов корпоративной сети и могут привести к следующим последствиям:

- Уничтожению (разрушению):
  – технических средств обработки информации;
  – носителей информации;
  – программного обеспечения (операционных систем, СУБД, прикладного программного обеспечения);

– информации (файлов, данных);
– помещений;
– персонала.

Показатель защищенности средств вычислительной техники (показатель защищенности) является характеристикой средств вычислительной техники, влияющей на защищенность и описываемой определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

Однако оценить весовые коэффициенты каждой угрозы достаточно затруднительно из-за высокой латентности их проявлений и отсутствия необходимой статистики. На основе анализа в области компьютерных преступлений, проводимого различными специалистами, все виды угроз электронной безопасности ранжируются по частоте проявления следующим образом:

- Кража (копирование) программного обеспечения.
- Подмена (несанкционированный ввод) информации.
- Уничтожение (разрушение) данных на носителях информации.
- Нарушение нормальной работы:
  - прерывание в результате вирусных атак;
  - перегрузка каналов связи.
- Модификация (изменение) данных на носителях информации.
- Перехват (несанкционированный съем) информации.
- Кража (несанкционированное копирование) ресурсов.
- Непредсказуемые потери.

Несмотря на предложенную классификацию для простоты считают, что каждая угроза может себя рано или поздно проявить и поэтому все они равны, т. е. при построении модели принято, что весовые коэффициенты каждой угрозы равны 1 (единице).

Описание состава угроз безопасности информации не решает проблемы моделирования их воздействия, в том числе и с учетом модели нарушителя разграничения доступа.

Модель нарушителя разграничения доступа рассматривается в качестве абстрактного (формализованного или неформализованного) описания нарушителя правил разграничения доступа.

Нарушителем правил разграничения доступа выступает субъект доступа, осуществляющий несанкционированный доступ к информации.

Все виды угроз по-разному проявляются в каждой точке корпоративной сети. В связи с этим оценивается наибольшая опасность и угроза в каждой точке корпоративной сети. Наложение угроз безопасности информации на модель корпоративной сети позволяет в первом приближении оценить их опасность и методом исключения определить наиболее актуальные для конкретного объекта варианты защиты. Кроме того, можно в первом приближении оценить объемы необходимых работ и выбрать магистральное направление по обеспечению защиты информации.

Следствием реализации выявленных угроз безопасности информации в конечном счете может стать ущемление прав собственника (пользователя) информации или нанесение ему материального ущерба, наступившее в результате:

- Уничтожения информации:

– из-за нарушения программных, аппаратных или программно-аппаратных средств ее обработки или систем защиты,

– форс-мажорных обстоятельств,

– применения специальных технических (например, размагничивающих генераторов), программных (например, логических бомб) средств воздействия, осуществляемого конкурентами, персоналом учреждения или его филиалов, преступными элементами или поставщиками средств обработки информации в интересах третьих лиц.

- Исчезновения (пропажи):

– информации в средствах обработки,

информации при передаче по телекоммуникационным каналам,

– носителей информации,

– персонала.

Первичный анализ приведенного перечня угроз безопасности информации показывает, что для обеспечения комплексной безопасности необходимо принятие как организационных, так и технических решений парирования.

Парирование угроз требует дифференцированного подхода к распределению материальных ресурсов, выделяемых на обеспечение информационной безопасности в зависимости от значимости угрозы, оценива-

емой весовыми коэффициентами, которые в конечном счете определяют показатель защищенности средств вычислительной техники и АС.

- Модификации или искажения информации в результате:

– нарушения программных, аппаратных или программно-аппаратных средств ее обработки или систем защиты;

– форс-мажорных обстоятельств;

– применения специальных программных (например, лазеек) средств воздействия, осуществляемого конкурентами, персоналом учреждения, поставщиками средств обработки информации в интересах третьих лиц.

- Хищения информации путем подключения к линиям связи или техническим средствам, за счет:

– снятия и расшифровки сигналов побочных ЭМИ;

– фотографирования;

– кражи носителей информации;

– подкупа или шантажа персонала учреждения или его филиалов;

– прослушивания конфиденциальных переговоров, осуществляемого конкурентами, персоналом учреждения или преступными элементами;

– несанкционированного копирования информации, считывания данных других пользователей;

– мистификации (маскировки под запросы системы);

– маскировки под зарегистрированного пользователя, проводимой обслуживающим персоналом АС;

– хищения информации с помощью программных ловушек.

- Махинаций с информацией путем:

– применения программных, программно-аппаратных или аппаратных средств, осуществляемых в интересах третьих лиц поставщиками средств обработки информации или проводимых персоналом учреждения;

– подделки электронной подписи или отказа от нее, нарушающих принципы защиты электронной подписи федеральным законом .[24]

---

[24] Федеральный закон "Об электронной цифровой подписи". Собрание законодательства Российской Федерации. № 2 от 14.01.02. Ст. 127.

3.1.2 Модель парирования угрозам безопасности

Уменьшить отрицательное воздействие угроз безопасности информации возможно различными методами. Среди них можно выделить следующие методы:

- Организационные.
- Инженерно-технические.
- Технические.
- Программно-аппаратные.

Организационные методы в основном ориентированы на работу с персоналом, выбор местоположения и размещения объектов корпоративной сети, организацию систем физической и противопожарной защиты, организацию контроля выполнения принятых мер, возложение персональной ответственности за выполнение мер защиты. Эти методы применяются не только для защиты информации и, как правило, уже частично реализованы на объектах корпоративной сети. Однако их применение дает значительный эффект и сокращает общее число угроз.

Инженерно-технические методы связаны с построением оптимальных сетей инженерных коммуникаций с учетом требований безопасности информации. Это довольно дорогостоящие методы, но они, как правило, реализуются еще на этапе строительства или реконструкции объекта, способствуют повышению его общей живучести и дают высокий эффект при устранении некоторых угроз безопасности информации. Некоторые источники угроз, например обусловленные стихийными бедствиями или техногенными факторами, вообще не устранимы другими методами.

Технические методы основаны на применении специальных технических средств защиты информации и контроля обстановки и дают значительный эффект при устранении угроз безопасности информации, связанных с действиями криминогенных элементов по добыванию информации незаконными техническими средствами. Кроме того, некоторые методы, например резервирование средств и каналов связи, оказывают эффект при воздействии некоторых техногенных факторов.

Программно-аппаратные методы в основном нацелены на устра-

нение угроз, непосредственно связанных с процессом обработки и передачи информации. Без этих методов невозможно построение целостной комплексной системы информационной безопасности.

Сопоставление описанных выше угроз безопасности информации и групп методов их парирования позволяет согласовать методы защиты по определенным методам угроз, а также определить соотношение в распределении средств, выделенных на обеспечение безопасности информации между группами используемых методов.

Анализ результатов моделирования, с учетом принятых в модели ограничений и допущений, позволяет заключить, что все группы методов парирования угрозам безопасности информации имеют примерно равную долю в организации комплексной защиты информации.

Эффективная защита информации осуществляется комплексом средств защиты.

Комплекс средств защиты представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения защиты средств вычислительной техники или АС от НСД к информации.

Однако необходимо учесть, что некоторые методы могут быть использованы только для решения ограниченного круга задач защиты. Это особенно характерно для устранения угроз техногенного и стихийного характера.

Наибольший эффект достигается при применении совокупности организационных и программно-аппаратных методов парирования.

Анализ весовых коэффициентов программно-аппаратных методов позволяет сделать вывод, что гипотетическое средство защиты корпоративной сети, прежде всего, должно обеспечивать разграничение доступа субъектов к объектам (мандатный и дискреционный принципы), управлять внешними потоками информации (фильтрация, ограничение, исключение) и, как минимум, обеспечивать управление внутренними потоками информации с одновременным контролем целостности программного обеспечения, конфигурации сети и возможности атак разрушающих воздействий.

3.2 Принципы построения системы информационной безопасности

Обеспечение безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу корпоративной сети. Это происходит из-за того, что любая система защиты, по определению, всегда налагает ограничения на работу организационного и технического характера.

Принцип максимальной дружественности. При формировании защиты корпоративных сетей не следует вводить запреты там, где без них можно обойтись. В случае введения ограничений сделать это с минимальными неудобствами для пользователя. При применении запретительных мер следует учитывать совместимость создаваемой системы комплексной защиты с используемой операционной и программно-аппаратной структурой корпоративной сети и сложившимися традициями фирмы.

Принцип прозрачности. Этот принцип требует, чтобы система защиты информации должна работать в «фоновом» режиме, быть «незаметной» и не мешать пользователям в основной работе, но при этом выполнять все возложенные на нее функции.

Принцип превентивности. Этот принцип основан на предупреждении угроз безопасности информации. Предупреждение угроз за счет создания системы комплексной защиты информации требует значительно меньших финансовых, временных и материальных затрат, чем затраты, вызванные потерей информации .

Принцип оптимальности. Оптимальный выбор соотношения между различными методами и способами парирования угрозам безопасности информации при принятии решения позволит в значительной степени сократить расходы на создание системы защиты.

Принцип адекватности. Принимаемые решения должны быть дифференцированы в зависимости от важности, частоты и вероятности возникновения угроз безопасности информации, степени конфиденциальности самой информации и ее коммерческой стоимости.

Принцип системного подхода к построению системы защиты позволяет заложить комплекс мероприятий по парированию угрозам безопасности информации уже на стадии проектирования корпоративной сети,

обеспечив оптимальное сочетание организационных и инженерно-технических мер защиты информации. Важность реализации этого принципа основана на том, что оборудование действующей незащищенной корпоративной сети средствами защиты информации сложнее и дороже, чем изначальное проектирование и построение ее в защищенном варианте.

Принцип адаптивности. По этому принципу система защиты информации строится с учетом возможного изменения конфигурации сети, числа пользователей и степени конфиденциальности и ценности информации. При этом введение каждого нового элемента сети или изменение действующих условий не должно снижать достигнутый уровень защищенности корпоративной сети в целом.

Принцип доказательности. При создании системы защиты информации необходимо соблюдение организационных мер внутри корпоративной сети, включая привязку логического и физического рабочего места друг к другу и применения специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации на основе сравнения различных уровней или так называемой верификации.

Верификация означает процесс сравнения двух уровней спецификации средств вычислительной техники или АС на надлежащее соответствие.

Реализация принципа доказательности позволяет сократить расходы на усложнение системы, например, применять цифровую электронную подпись только при работе с удаленными и внешними рабочими местами и терминалами, связанными с корпоративной сетью по каналам связи.

Все приведенные принципы должны быть положены в основу при выборе направлений обеспечения безопасности корпоративной сети, функций и мер защиты информации.

Определившись с функциями, которые должны быть реализованы для защиты информации на конкретном объекте, и приступая к выбору конкретных технических решений, то есть к выбору средств защиты информации, обязательно встает вопрос о подтверждении выполнения тех или иных функций конкретным средством защиты. Это немаловажный процесс, который в определенных случаях (например, при организации за-

щиты информации, содержащей государственную тайну или сведения о личности – персональные данные) строго регламентирован. Что же может явиться свидетельством того, что те или иные функции защиты реализованы конкретным средством защиты? Конечно же, сертификат соответствия – документ, которым независимые эксперты свидетельствуют о готовности средства выполнить эти функции.

Сертификация уровня защиты (сертификация) – процесс установления соответствия средства вычислительной техники или АС набору определенных требований по защите.

На основании сертификации выдается сертификат защиты или сертификат.

Сертификат защиты (сертификат) – документ, удостоверяющий соответствие средства вычислительной техники или АС набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

Глава 4. ЭЛЕКТРОННАЯ КОММЕРЦИЯ КАК ОДНО ИЗ УСЛОВИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ЗАКЛЮЧЕНИИ ДЕЛОВЫХ СДЕЛОК

4.1 Юридический статус электронной коммерции

Применение глобальных коммуникаций в коммерческой деятельности и повседневной жизни обусловило возникновение таких новых экономических и правовых явлений, как экономика в режиме реального времени (The on-line economy) и электронная коммерция (electronic commerce). Развитие экономики в режиме реального времени или электронной коммерции сопровождается быстрыми и значительными изменениями в сфере правового регулирования бизнеса. В законодательстве многих стран и в международном праве уже закреплены принципиально новые категории: электронная сделка, электронная подпись, электронные платежи, электронные деньги и т. д.

В юридическом смысле электронная коммерция представляет собой заключение на международных и внутренних рынках в компьютерной форме следующих сделок (но не ограничивается ими):

- куплю-продажу,
- поставку,
- соглашение о распределении продукции,
- деятельность торгового представительства или агентства,
- факторинг,
- лизинг,
- проектирование,
- консалтинг,
- инжиниринг,

- инвестиционные контракты,
- страхование,
- соглашения об эксплуатации и концессии,
- банковские услуги,
- совместную деятельность и другие формы промышленного и делового сотрудничества,
- перевозку грузов или пассажиров всеми видами транспортных средств.

Число сделок, совершаемых электронным способом, растет (объем торговли с использованием Интернета в настоящее время удваивается каждые сто дней).

В этой связи возникают вопросы с точки зрения юриспруденции:

- Какие правовые подходы и методы необходимо использовать, чтобы оперативно и эффективно отреагировать на появление новых возможностей для бизнеса?
- Какие существуют в настоящее время наиболее серьезные правовые препятствия для осуществления этих возможностей и наиболее действенные способы их преодоления?

С точки зрения ответов на эти вопросы важным является условие, позволяющее с точки зрения права широко использовать электронную цифровую подпись. С юридической точки зрения это выражено правовыми определениями, данными в законе «Об электронной цифровой подписи». В соответствии с этим законом законодательно закреплены такие понятия как:

- Владелец сертификата ключа электронной цифровой подписи.
- Закрытый и открытый ключ электронной цифровой подписи.
- Подтверждение подлинности электронной цифровой подписи в электронном документе.
- Пользователь сертификата ключа электронной цифровой подписи.
- Сертификат ключа цифровой подписи.
- Сертификат средств электронной цифровой подписи.
- Средства электронной цифровой подписи.
- Электронный документ.
- Электронная коммерция.
- Электронная цифровая подпись.

Владельцем сертификата ключа электронной цифровой подписи считается физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи (ЭЦП), позволяющим с помощью средств такой подписи создавать свою ЭЦП в электронных документах. Это означает, что владелец сертификата ключа ЭЦП имеет право подписывать любые электронные документы.

Электронная цифровая подпись – это реквизит электронного документа, предназначенного для его защиты от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющего идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронных документах.

Электронный документ представляет собой документ, в котором информация представлена в электронно-цифровой форме.

С точки зрения безопасности ЭЦП важным является понятие открытый и закрытый ключ ЭЦП.

Закрытый ключ ЭЦП представляет собой уникальную последовательность символов, известную владельцу сертификата ключа ЭЦП и предназначенную для создания в электронном документе ЭЦП с использованием средств такой подписи.

Открытый ключ ЭЦП предназначен для подтверждения с использованием средств такой подписи ее подлинности в электронном документе и дает возможность при уникальной последовательности символов, соответствующих закрытому ключу подписи, доступа любому пользователю информационной системы.

С юридической точки зрения важным условием по обеспечению безопасности является условие подтверждения подписи как со стороны владельца этой подписи, так и лица, который должен удостовериться в надежности и подлинности электронного документа.

Подтверждение подлинности ЭЦП в электронном документе состоит в положительном результате проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности этой подписи в ЭД владельцу сертификата ключа подписи и отсутствия искажений в подписанном этой подписью электронном документе.

Проверку ЭЦП на ее подлинность может выполнить **пользователь сертификата ключа ЭЦП**, которым считается физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа такой подписи для проверки принадлежности этой подписи владельцу сертификата ключа ЭЦП.

Сертификат ключа ЭЦП представляет собой документ на бумажном носителе или электронный документ с ЭЦП уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ такой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа подписи.

Сертификат средств ЭЦП, в свою очередь, является документом на бумажном носителе, выданным в соответствии с правилами системы сертификации для подтверждения соответствия средств ЭЦП установленным требованиям.

Для обеспечения безопасности как владельца ЭЦП, так и лиц, которым необходим доступ к электронному документу, служат средства ЭЦП.

Средствами ЭЦП являются аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

- создание ЭЦП в электронном документе с использованием закрытого ключа такой подписи,
- подтверждение с использованием открытого ключа ЭЦП подлинности этой подписи в электронном документе,
- создание закрытых и открытых ключей электронного документа.

4.2 Стратегия электронной коммерции

Электронная коммерция – это заключение различных сделок на международных и внутренних рынках в компьютерной форме.

Электронная коммерция на современном этапе требует особой правовой стратегии, которая способствовала бы развитию глобального и открытого рынка. Такая стратегия, *во-первых*, должна опираться, прежде всего, на грамотное использование традиционных, базовых юридических норм и правил, а *во-вторых*, предусматривать создание новых, специализированных правовых институтов и процедур.

С точки зрения правовой защиты возникает необходимость унификации законодательства и упрощения правил и процедур, применяемых в различных странах, что требует сотрудничества бизнеса и государственной власти не только в пределах одного государства, но и на международном уровне.

В числе наиболее важных юридических вопросов, требующих неотложного решения с участием мирового сообщества, следует назвать:

- налогообложение;
- тарифы;
- требования к форме заключения сделок;
- ответственность;
- аутентификацию;
- защиту информации;
- охрану прав:
  - потребителя,
  - интеллектуальной собственности.

На международном уровне присутствует и иная точка зрения по рассматриваемому вопросу. Она состоит в том, что в связи с глобальным характером on-line economy законодательство должно быть сведено к минимуму, стать последовательно международным и прозрачным, соответствовать четко обозначенным целям, обеспечивать доверие, эффективность и унифицированные правила поведения.

Глобальный и разветвленный характер экономики в режиме реального времени делает невозможным ее регулирование каким-либо правительством или государственным органом. Как результат – предпочтителен метод саморегулирования.

Глобальный бизнес-диалог должен быть настроен на предложение ясных и конкретных решений и разработку правил или Кодексов поведения, относящихся к нормам саморегулирования в бизнесе, которые целесообразно формировать с учетом консультаций с правительствами государств и международными организациями.

Динамичность электронной коммерции предполагает относительно быстрые изменения «правил игры». Поэтому очевидно, что страны, где правовая система основывается на судебном прецеденте (наличии решения суда по аналогичному поводу), имеют некоторое преимущество в

оперативности по сравнению со странами, в которых применяются исключительно законодательные акты, принятие или изменение которых требует специальной процедуры и, следовательно, времени.

В настоящее время один из основных правовых принципов электронной коммерции состоит в том, что стороны, заключившие договор, не вправе ставить под сомнение законность и действительность последнего только на том основании, что он заключен электронным способом.

Добиться гарантированного соблюдения этого принципа не всегда возможно, что часто порождает значительные юридические сложности. В частности, положения такого соглашения не всегда обладают юридической силой в случае судебного разбирательства. Это связано с тем, что в законодательстве ряда стран предусматривается право сторон оспорить законность заключения того или иного соглашения на том основании, что требуется традиционный письменный договор, содержащий все его существенные условия, заключенный на бумаге и заверенный собственноручными подписями сторон. Отсюда следует, что электронная коммерция часто не в состоянии преодолеть правовые препятствия, которые могут возникать в силу общеобязательных положений национального закона.

С целью организации помощи странам в преодолении перечисленных правовых препятствий Комиссией Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) в 1996 г. был разработан примерный свод правил – Типовой закон «Об электронной коммерции» (Model Low On Electronic Commerce).

Закон представляет собой модель, с помощью которой страны могут в национальном законодательстве решить основные проблемы, связанные с юридической значимостью договоров, заключаемых при помощи ЭВМ, касающиеся:

- Обязательной электронной письменной формы, подписи, оригинала и копии.
- Хранения договорной документации в электронном виде.
- Признания электронной подписи в качестве судебного доказательства.

Правовой режим электронного обмена данными, предусмотренный в Типовом законе, основывается на принципе так называемого функцио-

нального эквивалента. Это означает, что в случае, когда национальный закон предписывает, чтобы действия, связанные с заключением и исполнением сделок, осуществлялись в письменном виде или с использованием письменных документов, требование считается выполненным, если указанные действия осуществляются посредством одного или нескольких электронных сообщений с соблюдением положений законодательства.

Предполагается, что, включив предусматриваемые Типовым законом процедуры в национальное законодательство для урегулирования тех ситуаций, когда стороны выбирают электронные средства передачи данных, государство тем самым создает правовую среду, нейтральную (без каких-либо предпочтений) по отношению к различным носителям информации.

После принятия Типового закона «Об электронной коммерции» в ЮНСИТРАЛ было выработано соглашение о продолжении работы над юридическими нормами и правилами, которые могли бы сделать более предсказуемыми процессы в сфере электронной коммерции, тем самым способствуя развитию торговли во всех регионах. Среди таких правил названы положения, регулирующие отношение к электронной подписи.

Быстрый рост числа сделок, заключаемых с помощью Интернета и других сетей, обусловил приоритетность рассматриваемого вопроса.

Доверие к электронной подписи является ключевым условием для заключения договоров и передачи вещных или иных прав посредством электронной связи.

Работа над цифровыми подписями может не ограничиться сферой торгового права и включить также общие вопросы гражданского и административного права.

В России в области права и в юридической практике последних лет электронный бизнес в целом был скорее воспринят, нежели отторгнут. Он попал в процесс общей модернизации российской правовой системы и нашел опору в следующих быстро сформированных юридических конструкциях:

- «электронный документ»,
- «электронная форма сделки»,
- «электронная подпись»,
- «электронные расчеты»,

- «система ведения реестра владельцев ценных бумаг, использующая электронную базу данных».

Тем не менее в ряде российских законодательных актов в настоящее время сохраняются и предписания об использовании традиционных бумажных документов, подписанных собственноручной подписью.

К тому же следует отметить общую неразвитость и фрагментарность правовых норм, затрагивающих приведенную форму бизнеса. Как и на международном уровне, эти нормы становятся юридическими барьерами электронной коммерции, которые могут возникать в силу общеобязательных положений национального закона, и препятствуют интеграции нашей страны в глобальный электронный рынок.

Избавиться от подобных препятствий можно за счет:

- более обстоятельного отражения в отечественном законодательстве процессов, происходящих в сфере электронной коммерции,
- осуществления оптимизации соотношения норм административного и частного права,
- разработки всех необходимых юридических критериев, предъявляемых к электронному обмену данными.

Решение этих задач возможно в результате создания ряда новых законов об электронной коммерции, призванных обезопасить права заключающих электронные сделки.

Приоритет среди них принадлежит российскому Закону «Об электронной цифровой подписи», поскольку использование электронной подписи уже сегодня оказывает влияние как на экономику, так и на права граждан.

Развитие законодательства в этой области идет по пути его гармонизации, установления общих принципов регламентации электронной подписи, что позволяет создавать на международном уровне правовую инфраструктуру электронной подписи.

Вместе с тем следует отметить, что новый мир сетей предъявляет непомерно высокие требования к государству и праву в области защиты интересов участников электронного коммерческого оборота.

Сегодня демократическое государство часто демонстрирует свое бес-

силие в мире электронных сетей, так как они не контролируются этим государством и позволяют каждому включиться в общедоступные глобальные процессы.

Попытки целенаправленного вмешательства государства в функционирование всемирной децентрализованной сети типа Интернет не дают желаемого результата. В этой новой сфере государство не имеет ни средств принуждения, ни монополии, ни власти, ни суверенитета.

Защита индивидуальных и общественных интересов только посредством разрешительных или запретительных мер больше не срабатывает в нематериальном мире сетей. Поэтому при разработке юридических норм, посвященных электронной подписи, стратегия государства, ориентированная преимущественно на властные предписания, должна быть заменена новыми подходами с выделением следующих постулатов:

- Предоставить право участникам рынка в новом социальном пространстве корпоративных сетей на самозащиту в случае невозможности демократического государства защитить в достаточной степени участников рынка; на применение технических средств самозащиты с использованием в каждом конкретном случае тех сетей, надежность которых, по мнению пользователя, максимальна. Ряд технических средств можно применять без какой-либо специальной регламентации. В этом случае государство обязано отказаться от ограничительного регулирования.
- Предусмотреть юридически равноправную многостороннюю систему безопасности каждого участника электронной связи за счет развития технологии в информационном обществе, позволяющей создать систему самозащиты.
- Исключить в юридических нормах противоречия с техническими средствами самозащиты.
- Образовать соответствующую нормативную инфраструктуру, призванную помочь юридическому или физическому лицу пользоваться инструментом самозащиты в виде цифровой подписи или других средств специального правового механизма. Именно в этой области законодателю следует дополнить систему самозащиты необходимыми юридическими гарантиями со стороны государства.
- Обеспечить неприкосновенность частной жизни и личной инфор-

мации юридических и физических лиц в ряду обязательных государственных гарантий.

Особую роль при разработке перечисленных подходов и механизмов в России, как и во всем мире, играет законодательное моделирование. Так, Модельный закон «Об электронной цифровой подписи» по инициативе Межпарламентской ассамблеи стран–участниц СНГ рекомендован к принятию.

Этот Модельный закон явился научно-практической базой для разработки Федерального закона РФ «Об электронной цифровой подписи».

В числе наиболее важных юридических вопросов следует назвать:

- налогообложение,
- тарифы,
- требования к форме заключения сделок.

Доверие к электронной подписи является ключевым условием для заключения договоров и передачи вещных или иных прав посредством электронной связи.

3 апреля 2000 г. в нашей стране вышел в свет проект закона «О регулировании российского сегмента сети «Интернет».

Глава 5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

5.1 Система экономической безопасности коммерческих организаций

В условиях переходной экономики государство само подталкивает негосударственный сектор к теневой деятельности. Это связано с тем, что налоговое законодательство остается несовершенным; процедуры получения различных свидетельств, сертификатов, сдачи отчетности связаны, как правило, со взяточничеством.

В целом практика деятельности коммерческих организаций свидетельствует об их повышенной уязвимости от противоправных действий со стороны различного рода организованных преступных групп и преступных сообществ. В этой связи обеспечение безопасности в сфере экономической деятельности коммерческих организаций и структур становится одним из базовых принципов их надежного, эффективного и стабильного функционирования.

Эту проблему следует рассматривать в контексте становления и развития системы обеспечения экономической безопасности различных государств, взаимодействующих в этой сфере деятельности, в целом, т.е. определения их объектов и субъектов, источников внешних и внутренних угроз, элементов и функций системы, критериев ее надежности и эффективности.

Несомненно, что система обеспечения национальной экономической безопасности должна основываться на существующем конституционном строе, стабильности экономического положения, приумножении

научно-технического и производственного потенциала, повышении жизненного уровня граждан, уменьшении имущественной дифференциации населения и смягчении возможных социальных конфликтов.

Система экономической безопасности коммерческих организаций состоит из основных и вспомогательных подсистем.

К **основным подсистемам** относятся:

- Экономическая разведка.
- Внутренняя безопасность.
- Безопасность зданий.
- Физическая безопасность.
- Техническая безопасность.
- Безопасность связи.
- Компьютерная безопасность.
- Защита коммерческой тайны.
- Психолого-социологическая подсистема безопасности.
- Противопожарная безопасность.
- Безопасность перевозок.
- Информационно-аналитическая безопасность.
- Радиационно-химическая безопасность.
- Пропагандистское обеспечение.
- Экспертная проверка механизма системы безопасности.

К **вспомогательным подсистемам** относятся:

- Оповещения.
- Действия в критических (чрезвычайных) ситуациях.
- Нормативные акты службы безопасности.
- Нормативные акты персонала коммерческой организации
- Режим встреч и переговоров.
- Взаимодействие с правоохранительными органами.
- Обучение персонала коммерческой организации требованиям соблюдения безопасности в сфере экономической деятельности.
- Обучение службы безопасности.

Основным содержанием подсистем экономической безопасности является совокупность научно обоснованных и апробированных на практике с учетом мирового и отечественного опыта мер, выполняемых в

строго установленном порядке для решения задач определенного типа, подразумеваемых самим названием подсистемы.

Остановимся на кратком описании предложенных основных и вспомогательных подсистем экономической безопасности.

5.1.1 Экономическая разведка

Подсистема экономической разведки в общей системе экономической безопасности коммерческих организаций является приоритетной и направлена на достижение конкурентного преимущества объекта.

Конкурентное преимущество является одним из базовых слагаемых успешного развития и функционирования любого субъекта экономики. Поддержание преимущества требует, чтобы фирма постоянно предпринимала раньше, чем ее соперники, шаги в сторону расширения своих источников преимущества и особенно в сторону их совершенствования.

В задачи подсистемы «экономическая разведка» входит организация получения своевременной достоверной информации для выработки руководством коммерческих организаций рациональных управленческих решений, соответствующих складывающейся обстановке, стратегическим целям и оперативным задачам и позволяющих избежать неудач в своей деятельности, полнее и эффективнее реализовать свой интерес в бизнесе.

Сбор, анализ и обработка всевозможной информации, представляющей интерес для коммерческой организации, является наиболее ответственным звеном не только системы обеспечения безопасности, но и маркетинга, так как на ее основе вырабатывается политика предприятия.

Ведущим принципом работы коммерческих структур в условиях рынка является стремление к получению большей прибыли. Оно ограничивается возможностью понести убытки. Напомним, что риск, как неустранимый элемент управленческого решения любого уровня, в экономике трактуется в качестве стоимостного выражения вероятностного события, ведущего к потерям. Риски тем выше, чем выше шанс получить прибыль.

Значимость и полнота полученной информации дает возможность более точно подойти к оценке риска вследствие отклонений разведан-

ных данных от оценки сегодняшнего состояния и будущего развития ситуации.

Эти отклонения могут быть позитивными и негативными.

В первом случае речь идет о шансах получения прибыли, во втором – о рисках.

Каждому шансу получить прибыль противостоит возможность убытков, что вызывает готовность экономического субъекта к постоянной модификации своей стратегии в рамках принятых критериев эффективности для приспособления к этой системной неопределенности.

Задача деятельности по сбору и оценке информации в отношении связей коммерческой организации предусматривает упреждающее выявление в их числе источников внешней угрозы безопасности, максимально снижая неопределенность стратегического риска. Предполагается, что такого рода информация должна:

- Свидетельствовать об истинных намерениях потенциальных и действительных партнеров по отношению к коммерческой организации.
- Содержать сведения о сильных и слабых сторонах конкурентов.
- Позволять:

– оказывать влияние на позицию заинтересованных лиц в ходе переговорного процесса;

– контролировать ход реализации и соблюдения партнерами достигнутых ранее договоренностей;

– сигнализировать о возможном возникновении кризисных (чрезвычайных) ситуаций.

- Выявлять несанкционированные каналы утечки конфиденциальной информации о защищаемой коммерческой организации через осведомленность о ней партнеров и конкурентов.

Информация по предполагаемым партнерам и конкурентам, предоставляемая для принятия решения руководству предприятия, должна содержать следующие сведения:

- Полное название, юридический адрес, телефон, факс.
- Имена руководителей, их послужной список, адреса.
- Информацию об участии в судебных и иных разбирательствах, залогах имущества, выдержки из газетных и журнальных публикаций и их оценка.

- Дату и номер регистрации (город и юридическая форма).
- Информацию о практике исполнения платежей (какие суммы, в какие сроки и с какими задержками).
- Банки, с которыми работает фирма, адреса и номера счетов.
- Сравнительные характеристики состояния фирмы за последние **три** года.
- Рассчитанные коэффициенты ликвидности, покрытия, прибыльности вложений, отношение основных средств к инвестициям и др.
- Выдержки из последнего балансового отчета, отчета о прибыли и убытках.
- Дочерние и родительские компании, филиалы и отделения.
- Деятельность (товары и услуги, экспорт-импорт, условия сделок).
- Партнеры, их характеристика.
- Вероятные связи в криминальной среде.

Подобная система получения перечисленных сведений является необходимым значимым и безотказным инструментом для обеспечения бесперебойного функционирования негосударственного. субъекта экономики любого уровня и специализации.

5.1.2 Обеспечение внутренней безопасности коммерческой организации

Большое значение имеет обеспечение внутренней безопасности коммерческой организации. Такое направление деятельности по обеспечению безопасности в сфере экономической деятельности предполагает, прежде всего, предупреждение проникновения в число персонала структур экономического шпионажа, организованной преступности и отдельных лиц, ставящих целью нанесение ущерба предприятию. Эти условия обеспечиваются применением комплексных методов изучения и проверки предполагаемого кандидата на работу с использованием современных психотехнологий, например, проверки на полиграфе.

Проверка кандидатов на работу осуществляется подразделением безопасности и кадровым аппаратом коммерческой организации.[25]

---

[25] Дадалко В. А., Румянцева Е. Е., Пешко Д. А. Теневая экономика и кризис власти: проблемы и пути решения. - М.: Армита-Маркетинг, Менеджмент, 2000. - 416 с.

Одну из составляющих системы внутренней безопасности занимает механизм выявления источников информации структур организованной преступности, промышленного шпионажа среди сотрудников самой коммерческой организации. Наряду с этой деятельностью осуществляется работа по обнаружению источников внутренней угрозы безопасности, периодической профилактической проверке персонала, служебному расследованию фактов подлога, хищений и иного ущерба.

Особое внимание уделяется предупреждению негативных процессов в коллективах, создающих серьезную угрозу безопасности, и которые могут привести к чрезвычайным происшествиям (ЧП). В виде ЧП могут выступать:

- конфликтные ситуации трудовых коллективов с администрацией,
- обострения отношений на национальной почве,
- угрозы забастовок,
- групповые нарушения общественного порядка и т.п.

Работа по выявлению и устранению причин и условий негативных процессов проводится специальными социально-психологическими методами, используются различные формы изучения общественного мнения и оказания на него благоприятного воздействия путем убеждения и согласования интересов конфликтующих сторон, а также применения административных дисциплинарных методов.

К лицам, посягающим на законные права и интересы коммерческого предприятия, применяются меры воздействия, адекватные характеру их действий и в соответствии с юридической квалификацией последних.

При реализации задач внутренней безопасности осуществляется необходимая координация и взаимодействие с органами внутренних дел и прокуратурой, особенно при выявлении признаков состава преступления.

Работа по обеспечению внутренней безопасности не должна, с одной стороны, страдать излишним доверием к персоналу, с другой – нагнетать на объекте обстановку всеобщей слежки и подозрительности.

5.1.3 Обеспечение криминологической безопасности зданий и сооружений

Подсистема обеспечения криминологической безопасности зданий и сооружений направлена:

- на недопущение несанкционированного проникновения на объекты,
- пресечение возможных диверсионно-вредительских актов.
- обеспечение сохранности материальных ценностей,
- разработку соответствующих защитных мероприятий на случай возникновения чрезвычайных ситуаций (ЧС) и угрозы захвата зданий,
- выявление и устранение предпосылок к ЧП при функционировании субъектов экономики.

Анализ криминогенной обстановки показывает, что в отношении негосударственных хозяйствующих субъектов экономики и их персонала организованными преступными группировками все шире используются жесткие методы диверсионно-провокационной деятельности, которая приобретает характер бандитско-террористических актов. С целью нанесения материального и морального ущерба, запугивания, подчинения руководства предприятий своим планам и замыслам, вымогательства, срыва на длительное время нормального функционирования объекта структурами организованной преступности применяются взрывы, поджоги, минирование, обстрелы, вторжения на объекты, их захват, пикетирование, блокирование, акты вандализма. В этой связи большое значение приобретают такие направления деятельности, как обеспечение *физической безопасности руководства и персонала*, в том числе и персональная охрана лиц, которым может угрожать непосредственная опасность, а также защита зданий, сооружений, финансовых и материально-технических ценностей, принадлежащих коммерческим организациям.

Проведенное А. Крысиным[26] изучение отечественной и зарубежной статистики несанкционированных проникновений на коммерческие объекты позволило исследователю сделать вывод о том, что около 50% вторжений совершено на объекты со свободным допуском персонала и клиентов,

---

[26] Крысин А. Деятельность коммерческих банков (фирм) в условиях роста террористической угрозы.// Частный сыск, охрана, безопасность. 1994. № 1. - С. 33.

25% – на объекты с пассивными ограничениями типа неохраняемых заграждений, 20% – на объекты с охраняемыми заграждениями, контролируемыми охранниками, постовыми, патрульными службами и с пропускной системой и лишь 5% – на объекты с особым режимом охраны, допуск на которые обеспечивается по усложненной пропускной системе, а в охране используются современные технические устройства.

5.1.4 Обеспечение физической безопасности

Подсистема **«физическая безопасность»** направлена на вскрытие и пресечение террористических актов в отношении руководства коммерческой организации, обеспечение защиты жизни и здоровья персонала и членов их семей от посягательств преступных сообществ и отдельных лиц, вынашивающих противоправные намерения. В отношении руководства коммерческой организации защитные мероприятия проводятся постоянно и включают в себя, например, такие меры, как закрепление за руководством персональной охраны, специальное оборудование служебных кабинетов, автотранспорта и других средств передвижения, легендирование программы перспективной работы и текущего распорядка дня и т.п.

В отношении персонала коммерческой организации защитные мероприятия проводятся в случаях выявления в отношении конкретных лиц преступных посягательств.

Особое место в этой подсистеме занимают меры при возникновении чрезвычайных обстоятельств, например, захвата заложников из числа сотрудников либо их похищения. Несомненно, что приведенные меры осуществляются только при условии тесного взаимодействия и координации действий службы безопасности коммерческой организации с подразделениями Министерства внутренних дел (МВД), Федеральной службы безопасности (ФСБ), прокуратуры.

5.1.5 Обеспечение технической безопасности коммерческой деятельности

Меры технической безопасности призваны ограничить возможность съема информации о коммерческой организации структурами экономической разведки, организованной преступности и отдельными лицами, вынашивающими противоправные намерения путем технического про-

никновения в служебные помещения. Помимо организационно-режимных мер, такая система должна предусматривать своевременное обнаружение внедрения шпионской техники путем систематического проведения силами компетентных специалистов инструментальных проверок помещений, где ведутся конфиденциальные переговоры и откуда возможен съем интересующей конкурентов информации.

5.1.6 Обеспечение безопасности связи

Подсистема «безопасность связи» предназначена для комплексной защиты от перехвата конфиденциальных сведений, передаваемых по системам телефонной, телеграфной, факсимильной, фельдъегерской, радио-, конференцсвязи, других средств оперативного управления.[27,28,29,30]

Конечно, в условиях России степень автоматизации экономической деятельности значительно уступает западным стандартам, поскольку большинство расчетных операций дублируется на бумаге, а обмен платежными документами в реальном времени затрудняется отсутствием единого механизма межбанковских коммуникаций и соответствующих правовых норм. Кроме того, относительная слабость механизмов защиты и отсутствие у нас в стране до недавнего времени юридической ответственности за компьютерные преступления стимулирует злоумышленников и способствует их безнаказанности. Следует также учесть, что в подавляющем большинстве случаев в банках эксплуатируются стандартные однотипные вычислительные средства. К таким средствам можно отнести:

- IBM-совместимые персональные компьютеры с операционной системой MS-DOS,
- локальные сети с программным обеспечением фирмы Novell,
- программы автоматизации банковской деятельности, написанные на языках Clipper, FoxPro или Paradox и т.д.

---

[27] Жуков А. В., Маркин И. Н., Денисов В. Б. Все о защите коммерческой информации. - М., 1992. - С. 5.

[28] Самотуга В. А., Андреев С. С. Коммерческая тайна и ее защита. - М., 1992.

[29] Вуе М., Морозов В. Информационно-коммерческая безопасность: защита коммерческой тайны. - СПб., 1993.

[30] Валий А. Радиоэлектронная борьба. - М., 1989.

Все эти средства хорошо документированы и в деталях известны профессионалам. Простейшие механизмы защиты таких изделий (если они используются) легко преодолимы.

Кроме того, предстоящая конкурентная борьба между коммерческими банками, вероятно, заставит эти банки ускорить техническую модернизацию. Это связано с тем, что некоторые банки уже выполняют безналичные расчеты в реальном времени по кредитным/дебетовым магнитным карточкам через сеть SprintNet и центры верификации.

В настоящее время существуют возможности подключения к международной банковской системе SWIFT.

Начинают функционировать клиринговые центры межбанковских расчетов.

Разрабатываются проекты создания систем передачи финансовых документов на государственном уровне.[31]

5.1.7 Обеспечение информационной защиты и компьютерной безопасности

Рассмотрим содержание подсистемы компьютерная безопасность.

К общей классификации угроз компьютерной системы в коммерческой организации относятся следующие виды угроз:

- Конфиденциальности данных и программ. Реализуются при НСД к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи. Полезная информация может быть получена и при перехвате электромагнитного излучения, создаваемого аппаратурой системы. Определенные сведения о работе компьютерной системы извлекаются даже в том случае, когда ведется наблюдение за характером процесса обмена сообщениями (графиком) без доступа к их содержанию.
- Целостности:

• баз данных, программ, аппаратуры. Целостность баз данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицирован-

[31] Финансы и безопасность. Интеллектуальный подход. - М.: Центр стратегического планирования, 1994. - С. 2...3.

ных платежных документов в ответ на законные запросы, активной ретрансляции сообщений с их задержкой. Кроме того, в системах обработки сообщений отсроченные сообщения могут доставляться нужному адресату ранее заданного момента доставки. Несанкционированная модификация информации о безопасности системы может привести к несанкционированным действиям (неправильный выбор маршрута или потеря передаваемых данных) или искажению смысла передаваемых сообщений; аппаратуры и аппаратных средств. Целостность аппаратуры может быть нарушена при ее повреждении, похищении или незаконном изменении алгоритмов работы.

• Доступности данных. Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Эта угроза реализуется захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации. Эта угроза может привести к ненадежности или плохому качеству обслуживания в системе и, следовательно, потенциально будет влиять на достоверность и своевременность доставки платежных документов.

• Отказа от выполнения транзитных акций. Такие угрозы возникают в том случае, когда легальный пользователь выполняет транзакции (передает или принимает платежные документы) в системе, а затем отрицает свое участие в них, чтобы снять с себя ответственность.

Оценка уязвимости компьютерной системы и построение модели воздействий предполагает изучение всех вариантов реализации перечисленных выше угроз и выявления последствий, к которым они приводят.

Заслуживает внимания перечень наиболее вероятных случайных происшествий и злоумышленных действий, которым следует руководствоваться при оценке степени уязвимости проектируемой или эксплуатируемой компьютерной системы на примере банка.

К происшествиям, связанным с *техническими причинами*, относятся:

• выход из строя дискового накопителя с повреждением диска,

• отказы:

– вызванные ошибками в программном обеспечении,

– повреждением магнитных носителей: магнитных лент, гибких дисков;

- электронных схем компьютеров и периферийного оборудования,

♦нарушения в сети электропитания: перенапряжения или импульсные выбросы, аварийное отключение электропитания, воздействие статического электричества,

♦ошибки при передаче данных по каналам связи,

♦повреждения кабелей связи при строительных работах или реконструкциях.

К происшествиям, связанным со *стихийными бедствиями*, относятся:

- пожар,
- затопление при аварии водопровода, отопления или канализации,
- разрушение ветхих элементов конструкции здания;
- прямое попадание молнии или наводка импульсных токов во время грозы.

К происшествиям, связанным с *действиями людей*, относятся:

♦ ненамеренное:

- заражение компьютера вирусом при использовании посторонней программы – игры, учебного пакета и т.п.,

- повреждение аппаратуры в результате случайных действий безответственных лиц: обрыв соединительного кабеля или повреждение аппаратуры при неосторожном поведении в помещении, где установлена компьютерная система;

♦ неправильные действия малоквалифицированного персонала при профилактике, техническом обслуживании или ремонте,

♦ ошибочные действия оператора при работе, приводящие к разрушению данных,

♦ неправильное обращение с гибкими дисками или другими магнитными носителями при их использовании или хранении.

При анализе угроз, вызванных *злоумышленными действиями*, целесообразно оценить их вероятные мотивы, цели и последствия, а также определить круг потенциальных инициаторов (субъектов) таких действий.

Основными действующими лицами могут быть сотрудники (нынешние и бывшие), клиенты, конкуренты, конкуренты клиентов и сотрудники государственных органов.

Согласно статистике компьютерных преступлений в финансовых учреждениях, основным их мотивом оказывается незаконное обогащение.

Причем чаще всего в качестве субъектов преступлений выступают бывшие сотрудники банков.

Значительно реже фигурируют такие причины, как месть обиженных сотрудников или завоевание престижа среди определенной группы специалистов.

Анализируя способы осуществления злоумышленных действий, следует различать субъекта действий и конкретных исполнителей. Так, например, для шпионажа или диверсии в роли агентов могут быть использованы сотрудники банка, его клиенты, обслуживающий персонал из внешних организаций, просто посторонние, то есть все те лица, которые могут получить доступ к компьютерной системе или ее элементам.

По характеру исполнения злоумышленные действия целесообразно разделить на **три** вида:

1. Действия, не связанные с проникновением исполнителей в помещения, где расположены компьютерные системы.

2. Действия с единичными проникновениями исполнителей в помещения компьютерных систем, которые, в свою очередь, подразделяются:

- на открытые (под видом посетителей, сотрудников коммунальных служб (уборщики, водопроводчики, телефонисты, электрики) и т.п.);
- негласные (в выходные дни или ночью).

3. Действия, которые предусматривают наличие исполнителей в среде сотрудников банка, его клиентов или поставщиков оборудования, постоянно работающих в помещениях компьютерной системы, а также постоянного обслуживающего персонала.

Следует отметить, что некоторые компьютерные преступления могут осуществляться с применением одновременно нескольких видов злоумышленных действий. Например, агент из постоянного обслуживающего персонала проводит разведку и добывает дубликаты ключей или кодовых комбинаций замков помещений, документацию, информацию о системе защиты; негласное посещение специалистов позволяет получить пароли доступа к системе, а собственно злоумышленное действие, направленное на уничтожение, искажение или копирование информации, будет выполняться извне.

Рассмотрим злоумышленные действия (атаки) против компьютерной системы. К ним можно отнести:

• Проникновение в систему:

– через внешний (например, телефонный) канал связи с присвоением полномочий одного из легальных пользователей с целью подделки, копирования или уничтожения данных. Реализуется угадыванием либо:

- подбором и выявлением паролей и протоколов через агентуру в банке,
- перехватом паролей при негласном подключении к каналу во время сеанса связи,
- дистанционным перехватом паролей в результате приема электромагнитного излучения;

– телефонную сеть при перекоммутации канала на модем злоумышленника после вхождения легального пользователя в связь и предъявления им своих полномочий с целью присвоения прав этого пользователя на доступ к данным.

• Копирование финансовой информации и паролей при негласном пассивном подключении к кабелю локальной сети или приеме электромагнитного излучения сетевого адаптера.

• Выявление паролей легальных пользователей при негласном активном подключении к кабелю локальной сети при имитации запроса сетевой операционной системы.

• Анализ графика при пассивном подключении к каналу связи или при перехвате ЭМИ аппаратуры для выявления протоколов обмена.

• Подключение к каналу связи в качестве активного ретранслятора для фальсификации платежных документов, изменения их содержания, порядка следования, повторной передачи, доставки с задержкой или упреждением.

• Блокировка канала связи собственными сообщениями, вызывающая отказ в обслуживании легальных пользователей.

• Отказ абонента от факта приема (передачи) платежных документов или формирование ложных сведений о времени приема (передачи) сообщений для снятия с себя ответственности за выполнение этих операций.

• Формирование ложных утверждений о полученных (переданных) платежных документах:

• скрытая несанкционированная передача конфиденциальной ин-

формации в составе легального сообщения для выявления паролей, ключей и протоколов доступа;

♦ ложное объявление пользователем себя другим пользователем (маскировка) для нарушения адресации сообщений или возникновения отказа в законном обслуживании;

♦ злоупотребление привилегиями супервизора для нарушения механизмов безопасности локальной сети;

♦ перехват ЭМИ от дисплеев серверов или рабочих станций для копирования информации и выявления процедур доступа:

- сбор и анализ использованных распечаток, документации и других материалов для копирования информации или выявления паролей, идентификаторов, процедур доступа и ключей,
- визуальный перехват информации, выводимой на экран дисплеев или вводимой с клавиатуры для выявления паролей, идентификаторов и процедур доступа,
- негласная переработка оборудования или программного обеспечения на фирме-изготовителе, фирме-поставщике, в месте складирования или в пути следования к заказчику с целью внедрения средств несанкционированного доступа к информации извне (программ-перехватчиков и «троянских коней», аппаратуры вывода информации и т.п.), а также уничтожения информации или оборудования (например, с помощью программ-вирусов, ликвидаторов с дистанционным управлением или замедленного действия и т. п.).

• Разрушение:

♦ информации или создание сбоев в компьютерной системе с помощью вирусов для дезорганизации деятельности банка. Реализуется загрузкой вирусов в систему в нерабочее время, подменой игровых программ, используемых сотрудниками банка в рабочих помещениях, или вручением сотруднику банка «подарка» в виде новой компьютерной игры или другой занимательной программы;

♦ оборудования, магнитных носителей или дистанционное стирание информации.

• Похищение:

♦ оборудования, в том числе отдельных плат, дисководов, дорогостоящих микросхем, кабелей, дисков, лент, с целью продажи. Вле-

чет за собой потерю работоспособности системы, а иногда и уничтожение данных;

♦ магнитных носителей с целью получения доступа к данным и программам.

• Считывание информации с жестких и гибких дисков (в том числе и остатков "стертых" DOS-файлов), магнитных лент при копирования данных:

- с оборудования на рабочем месте в нерабочее время,

- использованием терминалов, оставленных без присмотра в рабочее время,

- магнитных носителей, оставленных на столах или в компьютерах, столах, шкафах и т.д.,

- оборудования и магнитных носителей, убранных в специальные хранилища при их вскрытии или взломе.

• Внесение изменений:

♦ в данные и программы для подделки и фальсификации финансовых документов при включении компьютерной системы во время негласного посещения в нерабочее время;

♦ в данные, записанные на оставленных без присмотра магнитных носителях.

• Использование оставленного без присмотра оборудования в рабочее время.

• Негласное присоединение к портам компьютера мобильных телефонов сотовой связи и считывающих устройств для съема интересующей информации.

• Установка:

– скрытых передатчиков для вывода информации или паролей с целью копирования данных или доступа к ним по легальным каналам связи с компьютерной системой в результате негласного посещения в нерабочее время; посещения с целью ремонта, настройки, профилактики оборудования или отладки программного обеспечения; скрытной подмены элементов оборудования при оставлении их без присмотра в рабочее время,

– ликвидаторов замедленного действия или с дистанционным управлением (программных, аппаратных или аппаратно-программных с

исполнительным механизмом взрывного, химического, электрического или вирусного действия) с целью уничтожения информации или оборудования.

- Скрытное внедрение программ преодоления защитных механизмов системы (типа «троянских коней») для подделки, уничтожения или копирования финансовой информации или копирования данных при последующих негласных посещениях при замене микросхем ПЗУ в компьютерах или модификации операционных систем и систем управления базами данных.
- Изменения базы данных или отдельных файлов в пределах выделенных полномочий для подделки или уничтожения финансовой информации.
- Считывание или внесение изменений информации в базах данных или отдельных файлах с присвоением чужих полномочий с целью копирования, подделки или уничтожения финансовой информации в результате подбора паролей; выявление паролей при похищении или визуальном наблюдении.
- Использование программных средств с целью преодоления защитных свойств системы: использование включенного в систему терминала, оставленного без присмотра.
- Несанкционированное изменение своих полномочий на доступ или полномочий других пользователей в обход механизмов безопасности.
- Негласное изъятие магнитных носителей с последующим возвращением с целью копирования, подделки или уничтожения данных, в результате использования семантических связей между секретной и несекретной информацией с целью добычи конфиденциальных сведений.
- Извлечение информации из статистических баз данных в результате использования связей между секретной и несекретной информацией с целью добычи конфиденциальных сведений.

5.1.7.1 Защита компьютерных сетей при формировании коммерческой деятельности

Специалистами-практиками выделяются следующие основные направления защиты компьютерной системы субъекта экономики:

- Аппаратуры и носителей информации от похищения, повреждения

и уничтожения. Эта задача – часть общей проблемы защиты имущественных прав организации. Для борьбы с угрозами этого вида используется традиционный комплекс организационно-технических мероприятий:

- физическая охрана и ограничение доступа к аппаратуре и носителям данных;
- ограждение зданий и территорий;
- оборудование помещений замками, охранной сигнализацией, а также различные устройства, препятствующие похищению компьютерной аппаратуры, ее компонентов и узлов.

- Информационных ресурсов от несанкционированного:
  - использования. Для этого используются средства контроля включения питания и загрузки программного обеспечения, а также методы парольной защиты при входе в систему;
  - доступа. Обеспечивает защиту конфиденциальности, целостности и готовности (доступности) информации и автоматизированных служб системы.
- Устраняющих утечку по побочным каналам ЭМИ и наводок. Реализуется экранированием аппаратуры и помещений, эксплуатацией специальной защищенной аппаратуры, применением маскирующих генераторов шумов и помех, а также дополнительной проверкой аппаратуры на наличие компрометирующих излучений.
- Информации в каналах связи и узлах коммутации. Блокирует угрозы, связанные с пассивным подключением к каналу («подслушивание»), предотвращает активное подключение с фальсификацией сообщений или ретрансляцией истинных сообщений, а также препятствует блокировке каналов связи. Для защиты используются процедуры аутентификации абонентов и сообщений, шифрование и специальные протоколы связи.
- Юридической значимости электронных документов. При передаче документов (платежных поручений, контрактов, распоряжений) по компьютерным сетям необходимо обеспечить доказательство истинности того, что документ был действительно создан и отправлен автором, а не фальсифицирован или модифицирован получателем или каким-либо третьим лицом. Кроме того, существует угроза отрицания авторства отправителем с целью снятия с себя ответственности за передачу

документа. Для защиты от таких случаев в практике обмена финансовыми документами используются методы аутентификации сообщений при отсутствии у сторон доверия друг к другу. Документ (сообщение) дополняется так называемой «цифровой подписью» – специальной меткой, неразрывно логически связанной с текстом и формируемой с помощью секретного криптографического ключа. Подделка таких меток без знания ключа посторонними лицами исключается и неопровержимо свидетельствует об авторстве. Нарушитель также не может отказаться от авторства документа.

- Автоматизированных систем от компьютерных вирусов и незаконной модификации. Реализуется применением иммуностойких программ и механизмов обнаружения фактов модификации программного обеспечения.

5.1.8 Обеспечение защиты коммерческой тайны

Подсистема «защита коммерческой тайны» в общей проблеме безопасности в обстановке конкурентной борьбы занимает одно из ключевых мест в обеспечении безопасности как коммерческой, так и предпринимательской деятельности.

В специальной литературе встречается разная трактовка понятия коммерческой тайны. Под коммерческой тайной в ряде случаев понимают форму обеспечения безопасности наиболее важной коммерческой информации, предполагающую ограничение ее распространения. В этом случае коммерческая информация рассматривается как сведения, связанные с производством, используемой технологией изготовления продукции, управлением, финансами и другой деятельностью предприятия.

В работе коммерческая тайна рассматривается как сведения, не являющиеся государственными секретами, но связанные с производством, технологией, НИОКР, управлением, финансами и другой деятельностью предприятия, разглашение которых может нанести ущерб его интересам.

В Акте о коммерческой тайне, одобренном в 1979 г. Американской ассоциацией юристов и принятом во многих штатах, коммерческая тайна трактуется как информация, включающая формулу, состав, комбинацию, программу, приспособление, метод, технику или процесс.[32] В этом

[32] Практика защиты коммерческой тайны в США. - М., 1992. - С.32...42.

случае информация, во-первых, имеет самостоятельную экономическую стоимость (используемую или потенциальную) благодаря тому, что не является общеизвестной или доступной людям, которые могут использовать ее в коммерческих целях. Во-вторых, является объектом разумных при определенных условиях усилий по защите информации.

Рассматривая различные точки зрения на определение понятия коммерческой тайны, следует отметить, что каждая из них в обязательном порядке предусматривает наличие определенного рода сведений, свободная циркуляция которых может нанести ущерб предприятию или его партнерам.

Для негосударственных предприятий такие сведения не могут быть отнесены к категории военной или государственной тайны, разумеется, за исключением случаев, когда частная фирма привлекается к выполнению особо важных государственных и оборонных заказов.

Исходя из действующих норм российского законодательства, перечень сведений, составляющих коммерческую тайну, определяется руководителем предприятия. Так, в соответствии с Постановлением Правительства России № 35 от 5 декабря 1991 г. в целях обеспечения деятельности государственной налоговой службы, правоохранительных и контролирующих органов запрещено относить к коммерческой тайне учредительные документы и устав предприятия, документы, дающие право заниматься предпринимательской деятельностью, сведения по установленным формам отчетности о финансово-хозяйственной деятельности, о платежеспособности и ряд других документов. Такое ограничение представляется довольно необоснованным по нескольким причинам. Во-первых, оно противоречит нормам ГК РФ 1994 г., во-вторых, из фабулы Постановления Правительства следует, что пользователями нижеперечисленных сведений могут быть исключительно государственные контролирующие и правоохранительные органы, а не широкий круг физических и юридических лиц.

Возникает ряд естественных вопросов:

1. Почему правоохранительные органы, налоговая инспекция, контролирующая структуры в пределах их компетенции, не могут быть допущены к сведениям, составляющим коммерческую тайну предприятия?

2. Что мешает руководству частной фирмы отнести необходимый блок

сведений о предприятии к коммерческой тайне, оговорив внутренним нормативным актом определенный порядок допуска к ней сотрудников МВД, прокуратуры, налоговой полиции и т.д.?

Представляется, что все же окончательное право и решение отнести информацию к составляющей коммерческую тайну должно оставаться за руководителем предприятия.

В силу этого под коммерческой тайной можно понимать любые сведения об экономической деятельности организации, силах и средствах ее обеспечения, допуск к которым документально ограничен соответствующим решением руководства субъекта, а разглашение сведений может способствовать нарушению надежного функционирования организации и невыполнению поставленных стратегических и тактических целей.

В этой связи защита сведений, составляющих коммерческую тайну организации, осуществляется с целью:

- Предотвращения возможных попыток неправомерного получения сведений, составляющих коммерческую тайну.
- Защиты конфиденциальной информации от угрозы со стороны организаций и отдельных лиц, ставящих своей целью подрыв безопасности объекта.
- Недопущения разглашения коммерческой информации персоналом предприятия. С этой целью организуется на коммерческом предприятии действенный и эффективный контроль действий персонала.

Защита организуется путем повсеместного применения договорной системы отношений с сотрудниками коммерческих организаций:

- при приеме на работу,
- изменении характера деятельности,
- увольнении.

Для обеспечения защиты в организации:

- Организуется специальное делопроизводство с соответствующим учетом документальных носителей сведений, составляющих коммерческую тайну.
- Устанавливается ограничительный порядок доступа к защищаемой информации, производится специальное оборудование помещений и хранилищ.

Обучение персонала осуществляется по адаптированным программам

согласно организационно-штатной расстановке и выполняемым служебным обязанностям.

Особое место в системе защиты принадлежит службе безопасности коммерческой организации, которая определяет каналы возможной утечки сведений, составляющих коммерческую тайну, и организует проведение специальных мероприятий по их перекрытию.

5.1.9 Формирование психолого-социологической устойчивости к чрезвычайным ситуациям и происшествиям

Психолого-социологическая подсистема криминологической безопасности обеспечивает соответствующую подготовку руководства и персонала коммерческой организации к ведению переговоров с партнерами, действиям в экстремальных ситуациях, развитие у них необходимых для выполнения служебных обязанностей морально-психологических качеств, чувства преданности фирме. Предусматривается также изучение морально-психологического климата среди сотрудников методами социологии, поддержание его на высоком уровне в целях повышения способности успешно противостоять внешним и внутренним угрозам безопасности, оценка психофизиологического состояния сотрудников, профилактика негативных процессов в коллективе, могущих способствовать правонарушениям.

5.1.9.1 Обеспечение психологической надежности работника, занимающегося коммерческой деятельностью

Одним из наиболее важных направлений профилактики ЧС и обеспечения надежности работника, занимающегося коммерческой деятельностью, является профессиональный отбор в виде медицинского и медико-психологического обследования кандидатов и психофизиологического анализа их возможностей.

Знание психологии позволяет разработать оптимальные режимы труда специалистов в течение дня, недели и даже года, по характеру деятельности и т.д.

Основу мероприятий составляет работа по обеспечению психологической надежности, включающая профилактику тяжелых форм утомле-

ния, запредельных форм психического напряжения и организацию соответствующих осмотров с ограничением допуска лиц с психическими состояниями, снижающими надежность работы специалиста в обычных и экстремальных условиях.

Непосредственно к этому направлению относятся: свойства личности и проблемы риска, кризисные ситуации и профилактика паники, контроль психического состояния человека в процессе труда руководителем, медицинскими работниками, техническими средствами.[33]

В структуре психологической деятельности человека различают три основные группы компонентов:[34]

- Психические процессы.
- Психические свойства.
- Психические состояния.

Психические процессы составляют основу психической деятельности любого человека. Без них невозможно формирование знаний и приобретение жизненного опыта. Различают следующие виды таких процессов:

- познавательные,
- эмоциональные,
- волевые психические (ощущения, восприятия, память и др.).

Психические свойства (качества личности) или свойства личности – это ее существенные особенности (направленность, характер, темперамент).

Среди качеств личности выделяют:

- интеллектуальные,
- эмоциональные,
- волевые,
- моральные,
- трудовые.

Свойства устойчивы и постоянны.

Психические состояния различаются разнообразием и временным характером, определяют особенности психической деятельности в конкретный момент (период) и могут как положительно, так и отрицательно

[33] Левин А. Секрет фирмы. - М., 1993.

[34] Барабаш В. И. Психология безопасности труда в промышленности. - Л.: ЛДНТП, 1984.

сказываться на течении всех психических процессов, протекающих в организме человека.

Исходя из задач психологии труда и проблем психологии безопасности труда, целесообразно выделять производственные психические состояния, имеющие особое значение в организации профилактики аварийности и производственного травматизма и характеризуемые работоспособностью.

Эффективность деятельности (работоспособность) человека базируется на уровне психического напряжения (стресса).

5.1.9.2 Формы психического напряжения

Психическое напряжение оказывает положительное влияние на результаты труда до определенного предела.

Превышение критического уровня активности ведет к снижению результатов труда вплоть до полной утраты работоспособности.

Чрезмерные формы психического напряжения обозначаются как запредельные. Нормальная загрузка (эмоциональная стимуляция) оператора не должна превышать 40...60% максимальной нагрузки, т.е. нагрузки до предела, когда наступает снижение работоспособности.

Запредельные формы психического напряжения вызывают дезинтеграцию психической деятельности различной выраженности, что в первую очередь ведет к снижению индивидуально свойственного человеку уровня психической работоспособности.

В более выраженных формах психического напряжения утрачиваются живость и координация действий, могут появляться непродуктивные формы поведения и другие отрицательные явления.

В зависимости от преобладания возбудительного или тормозного процессов можно выделить два типа запредельного психического напряжения – тормозной и возбудимый.

Тормозной тип характеризуется скованностью действий. Специалист не способен с прежней ловкостью выполнять профессиональные действия. Снижается скорость ответных реакций. Замедляется мыслительный процесс, ухудшается воспоминание, появляется рассеянность и другие отрицательные признаки, не свойственные конкретному человеку в спокойном состоянии.

Возбудимый тип проявляется в гиперактивности, многословности, дрожании рук и голоса. Человек в таком состоянии совершает многочисленные действия, не диктуемые конкретной потребностью. Он поправляет одежду, растирает руки, совершает многочисленные, не свойственные характеру деятельности движения. В общении с окружающими такой человек обнаруживает раздражительность, вспыльчивость, не свойственную ему резкость, грубость, обидчивость.

Таким образом, запредельные формы психического напряжения лежат в основе ошибочных действий и неправильного поведения человека в сложной обстановке. Длительное психическое напряжение и особенно их запредельные формы ведут к выраженным состояниям утомления.

В этой связи необходима организация контроля психического состояния операторов, коммерческих работников в связи с возможностью появления у таких специалистов особых психических состояний, которые не являются постоянными свойствами личности, но, возникая спонтанно или под влиянием внешних факторов, могут существенно изменить работоспособность этой личности.

Среди особых психических состояний, имеющих значение для психической надежности коммерческой деятельности, необходимо выделить:

- Пароксизмальные расстройства сознания.
- Психогенные изменения настроения.
- Состояния, связанные с приемом психически активных средств (стимуляторов, транквилизаторов, алкогольных напитков, наркотических средств и др.).

Пароксизмальные состояния – группа расстройств различного происхождения (органические заболевания головного мозга, эпилепсия, обмороки), характеризующихся кратковременной от секунд до нескольких минут утратой сознания. При выраженных формах наблюдаются падения человека и судорожные движения тела и конечностей.

Пароксизмальные перерывы в коммерческой деятельности могут быть причиной губительных последствий, особенно для водителей автотранспорта в момент перевозки ценного груза, работников охранной службы и ряда профессий, связанных с финансовой деятельностью, например, кассиры.

Современные средства психофизиологических исследований позво-

ляют своевременно выявлять лиц со скрытой наклонностью к пароксизмальным состояниям.

Психогенные изменения настроения и аффективные состояния возникают под влиянием психических воздействий. Снижение настроения и апатия могут длиться от нескольких часов до одного-двух месяцев. Снижение настроения происходит при гибели родных и близких людей, после конфликтных ситуаций. При этом человек становится безразличным, вялым, у него наблюдается общая скованность, заторможенность, затруднение переключения внимания, замедление темпа мышления. Снижение настроения сопровождается ухудшением самоконтроля и может быть причиной ЧП, несчастного случая, ЧС.

Под влиянием обиды, оскорбления, производственных неудач могут развиваться аффективные состояния (аффект – взрыв эмоций). В состоянии аффекта у человека развивается психогенное (эмоциональное) сужение объема сознания. При этом наблюдаются резкие движения, агрессивные и разрушительные действия. Лица, склонные к аффективным состояниям, относятся к категории лиц с повышенным риском травматизации и не должны назначаться на специальности с высокой ответственностью.

Лекарственные и алкогольные изменения психического состояния связаны с употреблением психически активных средств.

Современная медицина располагает большим арсеналом психофармакологических средств, оказывающих влияние на психическую деятельность людей.

Практический опыт свидетельствует, что прием легких стимуляторов (чая, кофе) помогает в борьбе с сонливостью и может способствовать повышению работоспособности на короткий период. Однако прием активных стимуляторов (перветина, фенамина) на ответственных видах работ способен вызвать отрицательный эффект – ухудшается самочувствие, уменьшаются подвижность и скорость реакций.

Распространенное среди населения употребление транквилизаторов (седуксена, элениума) представляет особую проблему. Оказывая выраженное успокоение и предупреждая развитие неврозов, эти препараты могут снижать психическую активность, замедлять реакции, вызывать апатию и сонливость.

Пьянство, алкоголизм и прием наркотиков также представляют серьезную проблему для безопасности труда. Недопустимость употребления алкогольных напитков в рабочее время и отрицательное влияние их на работоспособность общеизвестны. По различным данным автомобильный травматизм в 40..60% случаев связан с употреблением алкоголя. Имеется сообщение, что смертельные случаи на производстве в 64% случаев обусловлены приемом алкоголя и ошибочными действиями погибших.

5.1.10 Обеспечение защищенности коммерческих организаций от факторов опасности

5.1.10.1 Противопожарная безопасность в коммерческих организациях

Подсистема противопожарной безопасности имеет исключительно важное значение из-за значительного потенциального ущерба, который может быть причинен коммерческой организации в результате пожара, вне зависимости от того, что явилось его причиной – акции преступных элементов или непреднамеренные действия персонала. Основным содержанием данной подсистемы является система охранно-пожарной сигнализации и пожаротушения, а также комплексный план неотложных действий при возникновении угрозы пожара. При этом крайне важно, чтобы система охранно-пожарной сигнализации и пожаротушения в соответствии с Правилами пожарной безопасности (ПББ) – 01-03 обеспечивала:[35]

- раннее выявление:
- повышения температуры выше заданных параметров,
- дыма, искрообразования или пламени;
- раннее обнаружение паров веществ, образующих с воздухом взрывоопасные смеси,
- оповещение сотрудников и дежурного персонала, обслуживающего стационарные, переносные и подвижные средства пожаротушения и взрывопредупреждения,
- дистанционное, автоматическое и ручное включение стационарных средств пожаротушения,

[35] Правила пожарной безопасности (ПББ)-01-03.

- эвакуацию персонала из служебных помещений,
- подготовку к применению носимых средств пожаротушения.

5.1.10.2 Обеспечение безопасности перевозок

Подсистема безопасности перевозок предусматривает меры по предупреждению и отражению преступных посягательств на денежные средства, ценные бумаги, драгоценности и иные материальные ценности НХС при их транспортировке. Определяются основные и запасные варианты организации перевозок (выбор маршрута и вида транспорта, определение количества транспортных средств и личного состава, организация охраны трассы, контроль за передвижением, легендирование и т.п.).

5.1.10.3 Радиационная и химическая безопасность коммерческой организации

Подсистема **«радиационно-химическая безопасность»** обеспечивает своевременное обнаружение и пресечение попыток криминальных элементов нанести ущерб коммерческой организации и ее персоналу с использованием радиоактивных и отравляющих веществ. Она также предусматривает профилактическое поддержание параметров воздушной среды на объекте в пределах требований установленных норм, постоянный мониторинг радиационного и химического загрязнения окружающей среды, обеспечение персонала средствами коллективной и индивидуальной защиты.

5.1.11 Информационно-аналитические методы обеспечения безопасности в коммерческих организациях

Информационно-аналитическая подсистема обеспечивает упорядоченное накопление, научно обоснованное обобщение и анализ информации по различным направлениям криминологической безопасности НХС с выделением как положительных, так и отрицательных тенденций процесса обеспечения безопасности, и на этой основе выработкой предложений по дальнейшему развитию данных тенденций либо их нейтрализации.

В качестве одного из вариантов функционирования информационно-аналитической подсистемы можно рассмотреть концепцию известного

американского специалиста в области обеспечения безопасности А. Паттокоса, получившую название «OPSEC» (Operation Security).

По утверждению автора метода, «OPSEC» является эффективным средством сокрытия намерений, планов, мероприятий, технологий, позволяет постоянно быть «на шаг впереди противника», что в промышленной сфере означает устойчивое поддержание конкурентоспособности производимой продукции, финансового состояния предприятия.

Суть метода в том, чтобы пресечь, предотвратить или ограничить утечку той части информации, которая может дать конкуренту возможность узнать или «вычислить», что осуществляет или планирует предприятие, и, в результате, опередить его на рынке. Процесс организации защиты информации по методу «OPSEC» проходит поэтапно.

Первый этап («Анализ объекта защиты») состоит в определении того, что необходимо защищать. На этом этапе проводится анализ:

- по выявлению:
  - информации, нуждающейся в защите,
  - наиболее важных элементов (критических) защищаемой информации;
- определению:
  - срока жизни критической информации (времени, необходимому конкуренту для реализации добытой информации),
  - ключевых элементов информации (индикаторов), отражающих характер охраняемой информации;
- классификации индикаторов в зависимости от функциональных зон предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, персонал фирмы, финансы, управление и т.д.).

В ходе *второго этапа* осуществляется «выявление угроз»:

- определяется, кого может заинтересовать защищаемая информация;
- оцениваются:
  - методы, применяемые конкурентами для получения этой информации,
  - вероятные направления использования слабых мест в существующей на предприятии системе обеспечения безопасности в конкретном случае;

– разрабатывается система мероприятий по пресечению действий конкурента.

На *третьем этапе* анализируется эффективность принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность, безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.п.) с целью:

– моделирования планируемых операций,

– составления хронологических описаний событий (или их функциональных связей), безопасность которых необходимо обеспечить. Для каждого события планируемой операции определяются индикаторы, которые могут служить отправными данными для выявления критической информации,

– определения возможных специфических источников информации, анализ которых может привести к выявлению индикаторов (статьи в прессе, пресс-релизы, телефонные разговоры по незащищенным каналам, небрежное отношение к черновикам, передача излишней информации в ходе ведения переговоров, а также установившиеся стереотипы, шаблоны в повседневной работе и процедурах и т.п.).

В ходе *четвертого этапа* на основе проведенных на первых трех этапах аналитических исследований определяются необходимые дополнительные меры по обеспечению безопасности. При этом перечень дополнительных защитных мер, позволяющих «закрыть» выявленные уязвимые направления, сопровождается оценкой затрат, связанных с применением каждой меры. Сопоставление ожидаемого снижения уязвимости и предстоящих затрат позволяет оценить экономическую целесообразность предлагаемых мер.

На *пятом этапе* руководящими лицами фирмы, компании, учреждения рассматриваются представленные предложения по всем необходимым мерам безопасности и расчет их стоимости и эффективности.

Шестой этап – этап реализации принятых дополнительных мер безопасности с учетом установленных приоритетов.

Седьмой этап заключается в осуществлении контроля и доводке реализуемых мер безопасности. При этом проверяется эффективность принятых мер, выявляются оставшиеся незащищенными или вновь возник-

шие уязвимые места. Реализуемые меры доводятся до оптимального уровня, вводится постоянный контроль их функционирования.

В работе[36] предпринята попытка показа информационно-аналитической работы на относительно узком ее направлении – промышленном шпионаже в отношении конкурентоспособных изделий. Заслуживает внимания предложенная авторами логическая схема и используемые методы прогнозирования направлений промышленного шпионажа в качестве необходимого условия организации эффективной защиты информации о конкурентоспособном изделии, обеспечения целенаправленной защиты и рационального распределения затрат на ее организацию. По мнению авторов, направления шпионажа определяются сведениями, характеризующими конкурентоспособность изделия, которые не могут быть получены другими (легальными) способами. Для определения таких сведений необходимо из общего перечня сведений, характеризующих конкурентоспособность изделия, исключить сведения, получаемые методами научно-технического прогнозирования. При этом общий перечень сведений, характеризующих конкурентоспособность изделия, считается известным и разработчику, и его конкуренту. Последнее предположение вытекает из требования полноты учета факторов, влияющих на успех конкурентной борьбы, всеми ее участниками, что приводит обе стороны к единому общему перечню сведений, определяющему конкурентоспособность нового изделия. Для разработчика эти сведения являются защищаемыми, а для его конкурента – добываемыми. Авторами предлагаются четыре метода научно-технического прогнозирования, позволяющие получить информацию упреждающего характера на основе следующих методов:

• Экстраполяция тренда и авторегрессии на основе математической обработки значений характеристики, принимавшихся на ретроспективном периоде развития, позволяют рассчитать численное значение характеристики на заданный момент времени и оценить точность прогнозирования. В основу прогноза закладывается очевидность того, что конкури-

---

[36] Иванов М. Н., Пахомов А. С. Подходы к прогнозированию направлений промышленного шпионажа в отношении конкурентоспособных изделий.// Вопросы защиты информации. 1992. № 2.

рующая фирма уже располагает информацией о предыстории развития нового изделия и сама может использовать методы экстраполяции в полном объеме. В случае эволюционного развития изделия методы экстраполяции дают высокую точность прогноза.

• Корреляционный анализ на основе математической обработки совокупности значений характеристик образцов – аналогов разрабатываемому, позволяет установить вид их взаимозависимости и по набору известных характеристик нового образца рассчитать значения неизвестных характеристик, являющихся объектом защиты. Конкурирующая фирма может использовать в качестве исходных данных характеристики, в том числе и собственных изделий того же класса, что и новое изделие. При условии сохранения принципов конструирования точность метода достаточно высока.

Опережающая информация на основе анализа темпов научно-технических публикаций и тематики патентования позволяет определить направления научно-технических прорывов, сформировать облик нового изделия.

Построение сценариев и морфологического анализа на основе совокупной информации о фирме-разработчике и рынках сбыта позволяет определить варианты облика нового образца и оценить диапазоны возможных значений его характеристик. Упреждающая информация носит в основном качественный характер. Ее ценность состоит в определении наиболее вероятных факторов, определяющих конкурентоспособность изделия и подлежащих уточнению и конкретизации.

Оценка точности прогнозирования лежит в основе следующих вариантов:

1. Высокая точность.

2. Невысокая точность вследствие отсутствия некоторых видов исходной информации.

Следовательно, отсутствующие виды исходной информации формируют вероятные направления промышленного шпионажа.

Таким образом, при прогнозировании следует учитывать следующие направления промышленного шпионажа:

- осведомленность конкурента о перечне сведений, характеризующих конкурентоспособность нового изделия,

- наличие у конкурента объективной научно-технической информации, позволяющей расчетными и логическими методами определить защищаемые сведения о новом изделии,

- ограниченная точность методов научно-технического прогнозирования, вызывающая необходимость добывать информацию, содержащую недостающие исходные данные для повышения точности расчетных методов, а также непосредственно сведения, определяющие конкурентоспособность изделия.

Обе рассмотренные схемы построения информационно-аналитической работы заслуживают внимания и могут использоваться для разумного применения в практической деятельности по обеспечению криминологической безопасности субъектов экономики.

5.1.12 Пропаганда как одно из условий обеспечения коммерческой безопасности

Подсистема пропагандистского обеспечения направлена на формирование в стране и за рубежом объективного мнения о субъекте, его руководстве и персонале, способствующего более эффективной производственной и финансовой деятельности, укреплению авторитета и доверия в органах государственной власти и управления, среди партнеров и клиентов.

Одной из важных составляющих системы обеспечения криминологической безопасности коммерческой организации является подсистема, предназначенная для *контроля механизма функционирования самой системы.* При этом необходимо учитывать, что при проверке в первоочередном порядке должно исследоваться соответствие деятельности по обеспечению криминологической безопасности нормативным актам Российской Федерации. Задействование рассматриваемой подсистемы призвано способствовать поддержанию на требуемом уровне работы подразделения безопасности коммерческой организации, оптимизации организаторской и управленческой деятельности, полному использованию имеющихся резервов, усилению исполнительской дисциплины персонала. Подсистема функционирует на основе принципов объективности, систематичности, своевременности, конкретности, целенаправленности. Используются такие методы, как наблюдение, обследование, эксперимент.

По результатам контрольно-проверочных мероприятий разрабатываются конкретные предложения по устранению имеющихся недостатков и оказанию практической помощи исполнителям в совершенствовании работы.

5.1.13 Вспомогательные подсистемы безопасности коммерческих организаций

Вспомогательные подсистемы выполняют задачи обеспечения функционирования основных подсистем.

К вспомогательным подсистемам относятся:

- Средства оповещения.
- Действия в критических ситуациях.
- Нормативные акты:
  - персонала коммерческой организации;
  - подразделения безопасности коммерческой организации.
- Обучение:
  - персонала коммерческой организации;
  - подразделения безопасности коммерческой организации.
- Режим встреч и переговоров; взаимодействие с правоохранительными органами.

Таким образом, обеспечение криминологической безопасности негосударственного субъекта экономики осуществляется на основе комплексного подхода. Это достигается эмпирической разработкой и практической реализацией ряда специальных мер, объединенных по функциональному предназначению в основные и вспомогательные подсистемы. Основные и вспомогательные подсистемы находятся в органичной неразрывной связи, предусматривают взаимозависимость и взаимоподстраховку. Рассматриваемая система безопасности предполагает привлечение всех сил и средств защищаемой коммерческой организации при управлении ею на основе централизованного руководства.

Глава 6. ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ

6.1 Обеспечение защиты коммерческой тайны

Одной из важнейших составляющих экономической безопасности коммерческих организаций является обеспечение защиты коммерческой тайны.

Под коммерческой тайной следует понимать наличие сведений об экономической деятельности предприятия, силах и средствах ее обеспечения, ограничение допуска к которым документально оформлено соответствующим решением руководства субъекта, а их разглашение может способствовать нарушению функционирования фирмы и невыполнению поставленных стратегических и тактических задач.[37]

Определение сведений, составляющих коммерческую тайну, представляет собой одно из центральных звеньев в системе мер, осуществляемых фирмой по защите своей интеллектуальной и иной собственности.

Неправильное или несвоевременное выделение предмета защиты может существенно снизить эффективность системы безопасности либо вообще свести ее на нет.

Предложить какие-то единые для всех фирм формулировки относительно коммерческой тайны в виде «Перечня сведений» не представляется возможным, так как это понятие покрывает достаточно широкую сферу их деятельности. Во всяком случае, за рубежом то, что является тайной одного предприятия, не обязательно является секретом другой организации.

---

[37] Рубанов В. А. Охрана коммерческих тайн в рыночных условиях.// Вестник Агентства Post Factum, 1990. № 11.

Вместе с тем определенные рекомендации методического плана могут быть полезны при решении рассматриваемого вопроса.

6.1.1 Этапы определения сведений о коммерческой тайне

Прежде всего руководству коммерческим предприятием целесообразно весь процесс определения сведений, составляющих коммерческую тайну, условно разделить на следующие этапы:

Первый этап – определение списка сведений, которые могут быть отнесены к коммерческой тайне.

Второй этап – определение мест и способов получения сведений, которые могут составить коммерческую тайну.

Третий этап – оценка собранных сведений и выбор таких из них, которые составят коммерческую тайну.

Четвертый этап – выработка правил формирования и использования сведений, составляющих коммерческую тайну.

На основе классификации элементов, составляющих коммерческую тайну предприятия, руководством разрабатывается «Перечень сведений», в который должны быть включены:

1. Производство. Сведения о структуре производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции:

- Структура кадров и производства.
- Характер производства.
- Условия производства.
- Организация труда.
- Сведения:
  - о производственных возможностях предприятия;
  - фондах отдельных товаров, выделяемых для поставок на экспорт.
- Данные:
  - о типе и размещении оборудования;
  - резервах сырья.
- Уровень запасов.

2. Управление:

- Сведения:

  – о применяемых оригинальных методах управления фирмой;

– подготовке, принятии и исполнении отдельных решений руководства фирмы по коммерческим, организационным, производственным, научно-техническим и иным вопросам.

3. Планы:

- развития предприятия,
- производства и перспективный,
- инвестиций предприятий,
- запасов и готовой продукции,
- закупок и продаж.

• Сведения:

◆ о планах предприятия:

- по расширению производства и другим коммерческим замыслам,
- расширению производства (кроме оговариваемых в переговорах),
- о проектах годовых и перспективных экспортно-импортных планов по внешнеэкономической организации,
- результатах выполнения экспортно-импортного плана за истекший год по внешнеэкономической организации,
- предполагаемом создании за границей смешанных обществ с участием отечественного капитала (до их официальной регистрации).

• Инвестиционные программы, технико-экономические обоснования и планы инвестиций.

• Планово-аналитические материалы за текущий период.

• Оперативные данные о ходе выполнения экспортно-импортного плана (без воспроизводства показателей плана) по внешнеэкономической организации.

• Объем предстоящих закупок по срокам, ассортименту, ценам, странам, фирмам.

• Сводные сведения об эффективности экспорта или импорта товаров в целом по внешнеэкономической организации.

4. Совещания:

• Сведения:

◆ о фактах проведения совещаний;

◆ целях проводимых совещаний;

◆ предмете и результатах совещаний и заседаний органов управления фирмы.

5. Финансы:

- Балансы и бухгалтерские книги.
- Сведения, раскрывающие плановые и фактические показатели финансового плана.
- Финансовое состояние.
- Сведения:
  - о неудовлетворительном финансовом состоянии организации;
  - финансовых операциях;
  - об условии и размере кредита, полученного у иностранной организации (фирмы);
  - о размерах запланированного кредитования;
  - плановых и фактических показателях финансового плана внешнеэкономической организации (без воспроизводства показателей экспортно-импортного плана);
  - вопросах кредитных и валютных отношений с иностранными государствами, фирмами;
  - планах коммерческой деятельности смешанных обществ с участием отечественного капитала.
- Имущественное положение.
- Стоимость товарных запасов.
- Бюджет.
- Обороты.
- Банковские:
  - операции;
  - связи.
- Специфика международных расчетов с инофирмами.
- Плановые и отчетные данные по валютным операциям.
- Состояние:
  - банковских счетов предприятия и производимых операций;
  - кредита (пассивы и активы).

  Уровень:
  - выручки;
  - доходов.
- Долговые обязательства.
- Размеры и условия банковских кредитов.

- Рамки предоставляемого предприятию кредита.
- Принципы и условия предоставления коммерческих и государственных кредитов.
- Источники кредитов и условия по ним.
- Генеральная линия и тактика в валютных и кредитных вопросах.
- Размер комиссионных.

6. Рынок:

- Оригинальные методы изучения рынка сбыта.
- Состояние рынков сбыта.
- Обзоры рынка.
- Результаты маркетинговых исследований.
- Сведения, содержащие выводы и рекомендации специалистов по стратегии и тактике деятельности организации.
- Те же сведения по использованию конъюнктуры товарных рынков.
- Рыночная стратегия.
- Коммерческие замыслы, коммерческо-политические цели фирмы.
- Сведения:
  - о времени выхода на рынок при закупках (распродажах) товаров и выборе фирм для ведения коммерческих переговоров;
  - продажах товара на новых рынках;
  - конкретных направлениях в торговой политике;
  - экономических и иных обстоятельствах целесообразности закупки на свободно конвертируемую валюту отдельных товаров (лицензий), раскрывающие максимальную степень заинтересованности заказчика в импорте.
- Политика внешнеэкономической деятельности в целом и по регионам.
- Оригинальные методы осуществления продаж.

7. Партнеры:

- Круг клиентов.
- Списки клиентуры:
  - представителей или посредников;
  - покупателей;
  - поставщиков и потребителей.
- Сведения:
  - о составе торговых и других клиентов;

- представителях и посредниках;
- поставщиках;
- потребителях;
- характеристике предприятий и организаций как торговых партнеров (основные производственные фонды, товарооборот, прибыли, кредиты и т.п.);
- финансовом состоянии, репутации или других данных, характеризующих степень надежности иностранной фирмы дли ее представителей как торгового партнера.

- Негласные компаньоны товариществ.
- Коммерческие связи.
- Карточки клиентов.
- Места закупки товаров.
- Данные:
  - о поставщиках и клиентах;
  - на клиентов в торговле и рекламе.
- Сведения по иностранным коммерческим партнерам.

8. Переговоры:

- Внутренний порядок проработки предложений отечественных и зарубежных партнеров.
- Сведения:
  - о получаемых и прорабатываемых заказах и предложениях;
  - фактах подготовки и ведения переговоров;
  - лицах, ведущих переговоры, руководстве фирм (их характеристика);
  - мероприятиях, проводимых перед переговорами;
  - ходе и результатах коммерческих переговоров и условиях внешнеторговых сделок, в том числе контрактов на шефмонтаж и оказание услуг;
  - цели и задачах отечественного заказчика, закупающего товар за рубежом;
  - содержании технических переговоров с представителями иностранных фирм (до подписания протоколов, соглашений и т. п.).
- Директивы по проведению переговоров, включая тактику, границы полномочий должностных лиц по ценам, скидкам и другим условиям.

• Документы и сведения, относящиеся к деловой политике и позиции организации по конкретным сделкам (структура продажной калькуляции, уровень выручки, уровень предложенных цен до определенного момента).

• Материалы и приложения к предложениям при прямых переговорах.

• Тактика переговоров с партнерами.

• Сведения, раскрывающие тактику ведения переговоров при заключении контрактов или соглашений на закупку (продажу) товаров, уровень максимально достижимых (уторгованных) цен, объемы имеющихся средств (фондов) и другие конкурентные материалы, используемые для повышения эффективности сделки;

9. Контракты:

• Условия:

◦ по сделкам и соглашениям;

◦ платежам по контрактам;

◦ контрактам, включая цены.

• Особые:

– условия:

◦ контрактов (скидки, приплаты, рассрочки платежей, опционы и т.д.),

◦ компенсационных сделок;

◦ сделки и условия платежа по бартерным операциям, условия.

• Сведения:

◦ об условиях фрахтования транспорта иностранных компаний и фирм под перевозку внешнеторговых грузов;

◦ об исполнении контрактов;

◦ о номенклатуре и количестве товаров по взаимным обязательствам, предусмотренным соглашениями и протоколами о товарообороте;

◦ об условиях фрахтования транспорта иностранных компаний и фирм под перевозку внешнеторговых грузов, если они отличаются от общепринятых условий фрахтования;

◦ о детальной расшифровке предмета лицензий при купле-продаже;

◦ порядке поддержания контактов с правоохранительными органами.

• Сведения по вопросам обеспечения внутренней безопасности фирмы:

- перечень коммерческих, организационных и технических данных, обеспечивающих приоритет фирмы;
- методы и средства защиты коммерческой тайны;
- содержание правового обеспечения защиты коммерческой тайны;
- методы дезинформации конкурентов;
- данные о партнерах и конкурентах.

Когда «Перечень сведений», составляющих коммерческую тайну, установлен, необходимо приступить к определению мер ее защиты.

Отечественный и зарубежный опыт подтверждает принципиальную важность установления ответственности предпринимателя за правильность определения и правомерность использования средств обеспечения сохранности коммерческой тайны.

Следует иметь в виду, что деятельность по определению и защите коммерческой тайны – весьма дорогостоящие мероприятия.

В США, например, расходы фирм на мероприятия по защите научно-технической информации ежегодно составляют в среднем 10...15 млрд долларов. В целом на подобные мероприятия американским предпринимателям приходится тратить до 20% от суммы всех их расходов на научно-исследовательские и опытно-конструкторские работы. Ни одна бережливая зарубежная фирма не приступит к финансированию новой дорогостоящей научно-технической или опытно-конструкторской разработки без гарантий сохранности коммерческой тайны.

Защиту коммерческой тайны следует рассматривать как комплекс организационных и технических мер, проводимых предпринимателем в целях предотвращения хищения, умышленной передачи, уничтожения и несанкционированного доступа либо утечки этих данных к конкуренту.

Утечку сведений, составляющих коммерческую тайну, необходимо рассматривать как неправомерный выход (устным, письменным или иным путем) подобной информации от конкретного сотрудника фирмы, которому эта информация была доведена либо стала известна по службе или работе.

Для правильного выявления каналов утечки конфиденциальной информации очень важно определить ее носителей и пути возможного их выхода из-под контроля предпринимателя.

В каждой конкретной фирме перечень таких носителей может иметь индивидуальный характер, что определяется спецификой ее производ-

ственной, научно-технической, коммерческой и иной деятельности, а также степенью развития связей фирмы с деловыми партнерами в государствах – участниках СНГ и за рубежом.

6.1.2 Носители информации

Можно выделить четыре основных вида носителей информации:

– человек,
– документ,
– изделие (предмет, материал),
– процесс.

Виды носителей информации выделены по принципу функционального назначения.

Человек как источник владения и распространения информации занимает особое место. Это связано с тем, что в процессе интеллектуальной деятельности он создает новые знания и другие носители информации. Он же является и потребителем информации, пользователем других ее носителей и в то же время распространителем информации.

Функциональное назначение *документа* целиком исчерпывается свойством носителя информации. Документ рассматривается как средство закрепления различным способом на специальном материале информации о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека. В период своего существования документ проходит определенные этапы: составление и оформление, размножение, пересылку, использование, хранение, уничтожение. Конкретное наполнение этих этапов зависит от типа документа. Документы оформляются на бумажных носителях, на микроформах, на магнитных носителях, на перфоносителях.

Изделие обладает свойством носителя информации в качестве вспомогательного побочного эффекта, который воспринимается непосредственно человеком или специальными устройствами. Основное функциональное назначение изделия заключается в удовлетворении других, неинформационных потребностей общества. Следует помнить, что для изделий установлены определенные стадии «жизненного цикла»: изготовление макетов и опытных образцов, испытания, серийное производство, эксплуатация и т.д.; каждая из них может сопровождаться различ-

ного рода излучениями, шумовыми, световыми и другими эффектами, которые являются демаскирующими признаками, раскрывающими защищаемые сведения.

Процесс как носитель информации обладает свойствами, присущими как документу, так и изделию. Например, радиосвязь, осуществляемая посредством радиоволн, предназначена специально для приема-передачи информации. Вместе с тем, в силу объективных законов распространения радиоволн в пространстве, информацию, переносимую ими, может кроме потребителя, кому она непосредственно предназначена, получить конкурент, имеющий в распоряжении технические средства для ее перехвата.

Разработку мероприятий по сохранению коммерческой тайны фирмы целесообразно осуществлять, соблюдая принцип комплексного перекрытия возможных каналов утечки и обеспечения равнозначной надежности защиты всех ее носителей. Для этого следует:

- Иметь четкую схему информационных потоков защищаемой информации, исходя из производственных и коммерческих связей и потребностей фирмы.
- Определить состав пользователей и материальных носителей этой информации в схеме информационных потоков.
- Выделить наиболее уязвимые участки с точки зрения ее утечки.
- Выявить силы и средства, формы и методы, которые позволили бы в рамках приемлемых затрат надежно защитить все используемые носители коммерческой тайны, не затрудняя при этом основной деятельности фирмы.

За рубежом разработаны и используются разнообразные подходы. Так, например, в мелких и средних фирмах Швейцарии вопросами обеспечения охраны коммерческой тайны занимается непосредственно руководство. В Швеции эти обязанности возложены, как правило, на ответственное должностное лицо по работе с кадрами. В Финляндии существует практика, когда для обеспечения безопасности деятельности фирмы выделяется специальный сотрудник. По законодательству Германии предприятие, обрабатывающее данные, которые собираются в качестве вспомогательных средств для деловых целей (например, данные о клиентах в торговле и рекламе, сведения об исполнении контрактов), имею-

щее, если этот процесс автоматизирован, пять сотрудников, и если не автоматизирован – не менее 30, должно назначить уполномоченного по охране данных, не подлежащих оглашению. Крупные западные фирмы, в особенности выполняющие большой объем научных исследований и разработок либо занятые производством высокотехнологического оборудования, практикуют создание специальных служб по защите своих коммерческих секретов.

Наряду с внутрифирменными структурами на Западе существуют различные частные бюро, которые оказывают помощь организациям и фирмам в вопросах охраны принадлежащей им тайны, в том числе предоставление охранников, установку и обслуживание охранного и сигнализирующего оборудования (в Финляндии), решение технических, правовых и организационных вопросов (в Германии).

Во Франции защитой интересов предприятий от актов недобросовестной конкуренции занимаются также кабинеты адвокатов, юридических консультантов, союзы предпринимателей и потребителей.

Различные подходы к сохранению коммерческих интересов позволяют руководству коммерческой фирмы предварительно оценить возможный ущерб фирмы при разглашении (утечке) сведений, составляющих коммерческую тайну, и принять окончательное решение о создании службы безопасности на основе имеющихся финансовых средств.

При формировании представления о величине ущерба от утечки сведений, содержащих коммерческую тайну, к конкуренту важно оценить его в стоимостном выражении. Для этого можно воспользоваться услугами имеющихся в фирме специалистов соответствующих подразделений: планово-экономических, научно-технических, производственных, служб маркетинга, снабжения и др.

Только после установления величины экономического ущерба, который может последовать при утечке коммерческой тайны к конкуренту, можно переходить к рассмотрению вопроса об организационно-штатных мероприятиях по обеспечению ее сохранности.

ГЛАВА 7. ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ И ЗАКОНОМЕРНОСТИ ВОЗНИКНОВЕНИЯ И ПРЕДУПРЕЖДЕНИЯ НЕСЧАСТНЫХ СЛУЧАЕВ

7.1 Понятия несчастного случая

В соответствии с законом[38] несчастный случай классифицируется как случай с работающим, связанный с воздействием на него опасного производственного фактора.

С другой стороны, можно заключить, что несчастный случай адекватен травме или смерти, которые произошли на производстве в результате неожиданного внешнего воздействия. Это определение подтверждает, что существуют общие и значительные особенности, характеризующие многообразие, различие по причинам возникновения несчастного случая и ущербу, нанесенному работнику, предприятию, а в некоторых случаях и государству. Следовательно, несчастный случай – понятие экономическое и с точки зрения права необходимо опираться на определение несчастного случая, на основе которого можно выделить общие и существенные особенности. С точки зрения правовой направленности необходимо разделить такие понятия, как несчастный случай, умышленные преступные действия, самоубийство или попытки подобного рода.

В соответствии с положением «Об особенностях расследования несчастных случаев на производстве в отдельных отраслях и организа-

[38] Закон Российской Федерации "Об основах охраны труда в Российской Федерации,/ Сборник законодательств Российской Федерации. № 29 от 19.07.99.

циях»[39] содержание понятия «несчастный случай на производстве» соответствует стандартному международному термину «профессиональный несчастный случай». С точки зрения производственной опасности можно выделить воздействие внешней среды, т.е. воздействие предметов или процессов среды, окружающей человека, которое наносит вред здоровью человека или его жизни.

Воздействия внешней среды можно охарактеризовать как непосредственное внешнее воздействие, приводящее к травмам или к органическим изменениям и функциональным нарушениям.

Примером непосредственного внешнего воздействия, приводящего к травмам, может служить криминогенная ситуация в коммерческой деятельности, падение тяжелых предметов на работника при их неправильном складировании, хранении на складе, травмирование оборудованием, оснасткой или предметами труда и т.д. Непосредственное внешнее воздействие может привести к органическим изменениям и функциональным нарушениям организма. Это возможно в результате отравления сильнодействующими ядовитыми веществами (СДЯВ), поражения химически активными или радиоактивными веществами, акустического воздействия, поражения электромагнитными полями и др.

Анализ несчастных случаев и ЧП дает возможность говорить о том, что они, как правило, происходят неожиданно. Это не означает, что эти случаи нельзя предвидеть или предсказать вероятность их возникновения. Например, если опасная зона оборудования часто открыта по халатности работающего или вовсе не имеет ограждения, то рано или поздно на этом рабочем месте произойдет несчастный случай или чрезвычайное происшествие.

Однако для пострадавшего будет все-таки неожиданным внешнее воздействие опасного производственного фактора (ОПФ) из-за неожиданности такого воздействия, да и неподготовленности к нему. В этом случае вред, нанесенный работнику, причинен неожиданно для самого пострадавшего. Но, рассматривая происшедший несчастный случай, можно заключить, что он полностью является закономерным следствием ошибки человека в своих действиях.

---

[39] Положение "Об особенностях расследования несчастных случаев на производстве в отдельных отраслях и организациях". Постановление Минтруда Российской Федерации № 73 от 24.10.2002.

В этом случае такое понятие, как *неожиданность,* является субъективным. Субъективность заключается в том, что выражает позицию лиц, которые сами способствовали возникновению несчастных случаев либо пострадали от него или стали свидетелями его. И тем не менее фактор неожиданности всегда должен включаться в понятие несчастный случай, чтобы при расследовании можно было отличить его от заранее спланированных, умышленных действий с целью причинить вред другим или даже самому себе.

Из этого также следует, что воздействие опасного вредного производственного фактора (ОВПФ), приведшее к травматизму, потере здоровья или смерти, никогда не может быть преднамеренным.

Встает ряд вопросов: «В какой мере НС является следствием воздействия, прямо или опосредованно (косвенно) вызванного ошибочными действиями рабочего?», «Что лежит в основе самих ошибочных действий?»

Анализ несчастного случая показывает, что основой неправильных поступков человека являются:

- Отвлечение внимания во время работы (посторонний неожиданный раздражитель: окрик, звук, свет, аномальная температура), разрушающее цикл действия работника.
- Ошибка:
  - внимания, следствием чего явилось неправильное (неадекватное трудовому процессу) действие или бездействие;
  - в действии, возникающая перед началом работы (неправильная установка оснастки, оборудования, средств труда);
  - при выполнении действий (запаздывание или опережение реакции на раздражитель, нарушение границ опасной зоны оборудования, отмеченной запрещающими знаками и др.).
- Воздействие внешних факторов, отличающихся по своим параметрам от нормативных значений (снижение видимости, изменение химического состава воздуха, радиоактивность и др.).
- Отсутствие или игнорирование коллективных или индивидуальных средств защиты;
- Факторы:

• чисто психического характера (отвлечение посторонними мыслями, воспоминаниями, стрессовое воздействие перед работой и т.д.);

• организационного характера (неправильный выбор рабочего места, рабочей позы, недооценка опасности и т.п.);

• разрушение цикла действия в связи с неожиданным воздействием несвойственных рабочему месту факторов.

Непосредственной причиной других несчастных случаев и ЧП являются неожиданно возникающие перебои, неисправности в работе техники и орудий труда. Внешне эти случаи вызваны вроде бы не ошибочными действиями работников. Однако при более глубоком анализе причин и обстоятельств, предшествующих несчастному случаю или ЧП, можно обнаружить упущения и небрежность в осмотре оборудования, уходе за ним, т.е. как раз то, что относится непосредственно к дефектам в действиях или, как в настоящее время говорят, – к «человеческому» фактору.

Все приведенное подтверждает значение психического фактора в возникновении несчастного случая и ЧП в зависимости от действий и поступков человека в процессе трудовой деятельности.

Что же лежит в основе действий и поступков человека в процессе трудовой деятельности?

В основе действий и поступков находится осознанность и целеустремленность. Если человек постоянно действует осознанно и целеустремленно, то несчастный случай или ЧП никогда не произойдет.

Это связано, в первую очередь, с тем, что *целеустремленными* считаются такие поступки, которые подготавливаются и выполняются осознанным решением и управляются волевыми психическими действиями.

Целенаправленными могут считаться и автоматически выполняемые действия, находящиеся под постоянным контролем и управлением сознания. Как только функции контроля и управления со стороны сознания исчезают, прерывается цикл действия, возникает возможность неправильных действий при неожиданном воздействии постороннего внешнего раздражителя или непроизвольного отвлечения внимания по другой причине и, как следствие, – несчастный случай или ЧП.

Неосознанные ошибочные действия возникают, как правило, из-за различного рода изъянов в управлении поступками или принципа антиципации – предвидения наступающих событий. Такого рода поступки

может совершить как человек, действия которого привели к НС или ЧП, так и пострадавший. Например, коммерческий работник, достающий какой-либо предмет с верхней полки стеллажа склада, по неосторожности или из-за потери координации в движениях роняет этот предмет. В результате этого работник, находящийся рядом, получает травму из-за падения предмета на него. В этом случае неосознанное действие исходило от первого работника. Хотя и второй работник косвенно оказался виновным, так как снятие предмета, находящегося на высоте, представляет определенную опасность и нахождение рядом с человеком, выполняющим спуск предмета, запрещено. А второй работник нарушил этот запрет. Так что и его поступок можно отнести к числу неосознанных поступков: пострадавший неосознанно или случайно оказался в опасной зоне, не считаясь с возможностью падения предмета с вышерасположенного яруса стеллажа склада.

Во многих случаях виновник и «жертва» выступают в одном лице. Например, рабочий, пострадавший от НС или ЧП из-за невыполнения правил безопасности или в связи с беспечностью в своей деятельности.

Реально НС или ЧП является следствием сочетания случайного и необходимого. Так, если на рабочем месте (РМ) имеется источник риска с его многочисленными ОВПФ, являющимися источниками повышенной опасности, меры по устранению которых не принимаются, то на этом РМ рано или поздно произойдет НС или ЧП. В то же время, если при выполнении работ работник постоянно проявляет беспечность или невнимательность, то вероятность того, что он будет травмирован, очень высока.

Случайным в проявлении НС или ЧП будет источник опасности. В другом случае, когда работник приступает к деятельности, будучи чрезмерно взволнованным, и как следствие, работает невнимательно, а его движения становятся неуверенными, то неизбежно возникнут ошибки в движении, что может создать условия для НС или ЧП.

Таким образом, основой закономерности возникновения НС или ЧП является диалектическое единство случайных и необходимых событий. Следовательно, учет диалектического единства случайных и необходимых событий и обстоятельств дает возможность заключить, что НС или ЧП можно избежать:

- При тщательном соблюдении требований безопасности на всех уров-

нях (от работника до руководителя), невзирая на любые условия и по отношению к любому лицу независимо от занимаемой должности, профессионализма, стажа работы и т.п.

• В результате своевременного контроля не только вещественных условий производственной среды, но и учета субъективных факторов, обусловливающих возможность возникновения несчастного случая и ЧП: индивидуальных особенностей и индивидуального состояния работника, психологической обстановки на РМ, изменяющихся условий и пр. Любые отклонения субъективных факторов даже при безукоризненных вещественных условиях деятельности могут вызвать несчастный случай или привести к ЧП.

Все это трактует необходимость разработки условий и методов по выполнению требований максимального устранения всех причин, способствующих возникновению несчастных случаев и ЧС на основе учета объективного и субъективного факторов.

7.2 Опасность. Подверженность опасности. Защищенность

С целью определения возможности воздействия на работника объективного и субъективного факторов необходимо привести краткую характеристику взаимосвязей, которые могут существовать между источником риска, объективно угрожающим человеку, и подверженности опасности, которая может проявиться в связи с ошибочными действиями при обслуживании такого источником риска.

Выяснение этих взаимосвязей является значимой задачей выполнения условия максимального устранения всех возможностей возникновения несчастного случая или ЧП. Игнорирование их часто срывает применение мероприятий по их предупреждению.

Рассматривая источник риска как объективный вещественный фактор, можно с уверенностью заключить, что он представляет собой исходный пункт воздействия производственной среды на человека – потенциальную опасность или источник опасности.

При современном уровне развития техники и организации производства некоторые виды источников опасности могут быть полностью устранены за счет технических средств безопасности, автоматизации и роботизации производственных процессов и т.д. В таких случаях техни-

ческие и технологические мероприятия позволяют устранить источник опасности, а следовательно, и избежать возникновения несчастного случая с работниками и ЧП.

Устранение опасности за счет внедрения технических мероприятий является самой совершенной формой обеспечения безопасности труда. Эти возможности возрастают по мере развития научно-технического процесса во всех сферах деятельности, в том числе и коммерческой.

Однако это не означает, что можно полностью устранить источники опасности на каждом рабочем месте.

Опасное и вредное воздействие большинства источников опасности пока еще может быть устранено или уменьшено установлением технологических регламентов, за счет рациональных условий эксплуатации оборудования, выработки правил поведения и соблюдения технологической и производственной дисциплины. Обычно это называется условным, временным устранением угрозы несчастного случая или ЧП. В этом случае эффективность предупреждения или предотвращение несчастного случая или ЧП зависит полностью от способности работников выполнять необходимые требования безопасности. К тому же даже при высоком уровне развития техники невозможно полное устранение источников опасности и ОВПФ.

Поэтому следует обратить повышенное внимание на субъективное состояние работающих людей на оборудовании, представляющем угрозу.

Источники опасности подразделяются на следующие виды: потенциальные и явные.

Явные источники опасности характеризуются параметрами одинаково опасных для каждого человека факторов и процессов, возможностью взаимодействия человека с этим источником, временем взаимодействия и условиями, в которых это взаимодействие произошло, а также видом последствий. Анализ явного источника опасности позволяет наметить необходимые соответствующие меры для его устранения, чтобы обеспечить надежную защищенность обслуживающего персонала.

Потенциальные источники опасности характеризуются неожиданным во времени и пространстве проявлением явной опасности и ее угрозой. Угроза выражается направленностью воздействия опасности и вероятностью ее проявления, что характеризует источник риска. Они

могут выступать в виде предметов, которые при определенных обстоятельствах становятся объектами вредных и опасных воздействий в результате неправильного поведения самих работающих людей или злоумышленных действий.

Любой элемент рабочего места может стать при определенных условиях потенциальным источником опасности, и это зависит исключительно от степени невнимательности, неосторожности, усталости или болезненного состояния работника, другими словами, от его психического состояния.

Следовательно, превращение предметов внешней среды в потенциальные источники опасности является как бы функцией, которая зависит от величины отклонения в состоянии рабочего, от той присущей каждому индивидууму нормы, составляющей психофизиологическое условие безопасного выполнения работы в выбранной области деятельности.

Потенциальные источники опасности и возникающие в связи с их воздействием на работающих приводят к несчастным случаям и ЧП, а это требует разграничения таких понятий, как опасность и подверженность опасности.

Опасность рассматривается как возможное воздействие различных факторов на человека, которое может проявиться во взаимодействии с объектом или работающим и в виде различных по тяжести последствий.

Подверженность опасности означает взаимное влияние личного и вещественного факторов рабочего места, которое создает возможность несчастного случая или возникновения ЧП. Дело лишь в том, для кого, когда и какой опасный фактор может считаться источником опасности, – все это в значительной степени зависит от личности работника, от определенной специфики его поведения в процессе труда, его субъективного состояния и обусловленных этими факторами поступков. Так, если человек непригоден для рассматриваемого вида работ, например из-за дефекта какого-либо органа чувств или чрезмерной скованности, то вероятность возникновения несчастного случая или ЧП у него значительно больше, чем у других лиц в той же самой обстановке.

Но точно также повышает вероятность возникновения несчастного случая или ЧП и неправильный подход по отношению к опасности (неосторожность и вытекающие из этого ошибки в поведении работника).

Аналогичным образом увеличивает вероятность возникновения НС и ЧП сильная усталость и эмоциональное возбуждение. Одним словом, любое состояние, мешающее концентрации психических процессов, необходимое для выполнения трудовой деятельности, увеличивает вероятность возникновения несчастного случая или ЧП.

Для одного человека могут быть опасными предметы, которые безопасны для другого человека. Если человек более подвержен воздействию явных источников опасности, значит, степень подверженности опасности у него значительно выше, чем у большинства работников. И, наоборот, есть такие лица, для которых подверженность опасности минимальна благодаря тому, что они в значительной мере способны концентрировать свое внимание, обладают большими защитными качествами организма, имеют крепкое физическое и психофизиологическое здоровье, способны соблюдать необходимые для определенного вида деятельности требования.

Таким образом, для безопасной работы требуется умение приспосабливаться к ее специфике. В свою очередь, для этого необходимо приобрести это умение. В выработке такого умения существенную роль играют следующие профилактические мероприятия:

- Выяснение:
  - индивидуальной пригодности работника (профотбор), т.е. соответствие в силу его способностей требованиям, которые выдвигаются трудовой деятельностью определенного рода;
  - его поведения на рабочем месте с условием осмотрительности и внимательности при выполнении работы.
- Определение:
  - степени опытности работника (профессиональной пригодности);
  - отношения работника к опасности;
  - осознания им опасности в опасных зонах и ситуациях;
  - понимания его защищенности мерами и средствами безопасности.

В понятие защищенность входит степень приспособленности работника к специфике условий труда.

Условия труда представляют собой совокупность факторов среды и

трудового процесса, оказывающих влияние на здоровье и работоспособность человека в процессе труда.[40]

Если подверженность опасности характеризуется условиями труда, в которых человек подвержен воздействию источников опасности, то защищенность означает, в какой мере он способен уберечь себя от этих источников опасности (факторов риска).

Защищенность от опасности зависит от многих факторов, обстоятельств и условий. Анализ этих факторов показывает, что есть факторы, не зависящие от воли человека. Например, насколько ловки его руки при выполнении тех или иных движений, есть ли склонность выполнять требования, заложенные в технологические регламенты или изложенные в инструкции, в том числе и по безопасности, обладает ли он осмотрительностью и т.д. Но есть и такие факторы, которые человек может выработать соответствующей тренировкой или обучением приспособляемости. Для уменьшения влияния этих факторов на защищенность следует, в первую очередь, найти причину повышенной подверженности опасности, выяснить, что оказывает отрицательное воздействие на человека. Только после этого можно найти методы, позволяющие ликвидировать такое нежелательное влияние на психическое состояние человека. Необходимо помочь ему в повышении защищенности за счет самодисциплины, специфической приспособляемости, расширения сферы самозащищенности,[41] обращая его пристальное внимание на то, что неправильное поведение, в особенности в сочетании с другими факторами, усиливающими риск опасности, увеличивают степень подверженности опасности.

Следует обратить внимание на то, что однажды пережитый несчастный случай, ЧП или условия, совпадающие с чрезвычайным событием, способны вызвать усиление степени подверженности опасности за

[40] Гигиена труда. Гигиенические критерии оценки условий труда по показателям вредности и опасности факторов производственной среды, тяжести и напряженности трудового процесса. Р. 2.2.755-99.

[41] Несоленов Г. Ф. Возможность расширения зоны самозащищенности.// Философские, технические, методические и социальные аспекты преподавательской, научной и практической деятельности в сфере сервиса: Межвуз. сб. науч. тр. Самара: МГУС СФ. 2002. №7. - С. 41…50.

счет повышения остаточного психического воздействия, и само это может стать причиной нового несчастного случая, ЧП. Так, человек, получивший однажды травму на какой-то определенной фазе рабочего движения, может постоянно испытывать при приближении аналогичной фазы непреодолимое чувство страха. Этот страх провоцирует появление замешательства, которое может проявиться в его неуверенных движениях, что приведет к ошибкам, связанным с выполнением таких движений, и, как следствие, может привести к новым несчастным случаям и ЧП.

В основе психологической подготовки любого персонала лежат методы, которые позволяют найти ответ на следующие вопросы:

- Кто из обслуживающего персонала и при каких обстоятельствах может подвергаться факторам риска в повышенной степени?
- В каком объеме и с каким постоянством воздействуют на индивидуум происходящие НС или ЧП и какое психологическое воздействие на него они оказывают?
- Какими методами и средствами можно повысить индивидуальную защищенность человека от воздействия факторов опасности?

На эти вопросы можно дать ответ, рассмотрев условия, которые позволяют выразить индивидуальную подверженность риску.

7.3 Факторы, усиливающие индивидуальную подверженность риску

Факторы, усиливающие подверженность людей риску, могут быть разделены на две группы:

- Факторы, устойчиво повышающие подверженность риску.
- Факторы, временно повышающие подверженность риску.

7.3.1. Факторы, устойчиво повышающие подверженность риску

В этой группе существует очень много факторов, которые могут повысить у работника подверженность опасности. Основными из таких факторов могут быть:

- Функциональные изменения в ЦНС или других органах, имеющие болезненный характер или вызывающие близкое к нему состояние.
- Различные изъяны органов чувств.

- Нарушение связи между сенсорными и двигательными центрами высших отделов нервной системы.
- Дефекты, возникающие в согласованности и координации движений.
- Неуравновешенность эмоциональных процессов.
- Пагубные пристрастия к алкоголю, наркотикам.
- Неудовлетворенность работой и отсутствие интереса к ней.
- Шантаж и угроза.

Функциональные изменения в нервной системе или других органах, имеющие болезненный характер или вызывающие близкое к нему состояние. Среди них различают ряд стойких патологических изменений, которые хотя и не вызывают полной нетрудоспособности, но воздействуют на поведение, повышая подверженность риску. К таким факторам, например, можно отнести сердечно-сосудистые заболевания, сахарный диабет, эпилепсию и др.

Все эти болезни могут способствовать изменению поведения человека частично непосредственно и частично косвенно. Непосредственное изменение поведения человека выражается в форме периодической слабости, недомогания, а косвенное – путем общего воздействия на психику (подавленность, депрессия, раздражительность). Изменение же поведения человека могут усиливать его подверженность опасности. Кроме того, следует различать такие патологические изменения функций нервной системы, которые хотя и не означают нетрудоспособности, но оказывают отрицательное влияние на поведение работника с точки зрения его безопасности (нервные симптомы: головная боль, бессонница и др.).

Повышение защищенности лиц, подверженных функциональным изменениям в нервной системе или других органах организма, может быть достигнуто в первую очередь постоянным врачебным наблюдением и необходимым лечением. К тому же при профессиональном отборе необходимо учитывать симптомы, подтверждающие подверженность функциональным изменениям в нервной системе или других органах организма и не допускать таких лиц к работам повышенного риска.

Различные изъяны органов чувств. К ним можно отнести частичную потерю зрения, слуха, осязания, обоняния, координации. Особо опасным является сокрытие потенциальным работником таких наруше-

ний при профотборе, так как такие изъяны чаще всего обнаруживаются после несчастного случая или ЧП. Разумеется, дефекты органов чувств могут иметь различную степень, однако даже минимальный дефект может повысить подверженность опасности. Но если работник сознает свой недостаток и его отрицательное воздействие на безопасность, то он вполне может снизить вероятность возникновения несчастного случая или ЧП. При этом большая роль принадлежит приобретению необходимых навыков и выработке умения распоряжаться своим вниманием. Немаловажное значение приобретают практические навыки, профессионализм и соблюдение культуры труда.

Нарушение связи между сенсорными и двигательными центрами высших отделов нервной системы. Вследствие таких нарушений работник не способен с должной быстротой и точностью реагировать на внешние раздражители, воспринимаемые органами чувств. Анализ несчастных случаев и ЧП показывает, что, как правило, такие нарушения играют главную роль в возникновении большинства несчастных случаев, ЧП или способствуют возникновению ЧС.

Подверженность фактору риска повышается при замедленной или чересчур поспешной реакции на внешний раздражитель, которая необходима для ответной двигательной реакции. Подобные нарушения согласованности между сенсорными и моторными процессами проявляются не только в поступках, но и в трудовой деятельности, включающей в себя сложные действия.

Указанные нарушения согласованности в сенсорных компонентах могут быть компенсированы благодаря правильному распределению внимания.

Работник должен научиться приспосабливаться управлять своими движениями и поступками в соответствии с воздействием внешних раздражителей. Это значит, что он должен научиться вовремя замечать эти раздражители, требующие изменения его деятельности, и своевременно реагировать на них с определенной точностью. Это значит, что у работника должно быть развито чувство антиципации. Большая роль в этом отводится соответствующему автоматизму в выполнении трудового процесса, отработке определенных навыков, позволяющих отвечать на воздействие внешних раздражителей не только с рефлекторной

уверенностью, но и с требуемой точностью, необходимой в определенный момент.

Дефекты, возникающие в согласованности и координации движений. Такие нарушения чаще всего появляются в координации точных и сложных движений рук, которые необходимо выполнять в особо ответственных видах трудовой деятельности. В повседневной жизни это называется неловкостью.

Мышцы, выполняющие те или иные движения, управляются из различных двигательных центров коры головного мозга. У многих людей деятельность этих центров протекает с недостаточной согласованностью. В результате чего при выполнении рабочих движений и операций возможен периодический разрыв в цикле действий: временами человек как бы теряется, некоторые движения он пропускает, но зато появляются лишние, ненужные для выполнения работы. В таких случаях несогласованность движений сочетается с дефектами внимания и состоянием эмоциональной стесненности. Стремление к повышенному вниманию в этих случаях нередко лишь усиливает дефекты движений.

Профилактикой несчастных случаев и ЧП при наличии у работника таких факторов является ограничение допуска к работам, в которых от точности координации движений зависит и степень риска.

Неуравновешенность эмоциональных процессов. К ним можно отнести повышенную эмоциональную неустойчивость, неожиданные смены радости и злобы, острые эмоциональные реакции на незначительные внешние раздражители. Все эти факторы усиливают подверженность человека опасности, угрозе и снижают его защищенность.

Вредное воздействие неуравновешенности эмоциональных процессов может иногда сказаться и опосредованно (косвенно). Например, в форме недомыслия, необдуманности поступков, простых поспешных действий. Поверхностный характер процессов и отсутствие широты мышления могут приводить к возникновению ошибок в деятельности.

С другой стороны, во многих случаях замедленность мышления мешает в критических ситуациях моментально изменить действия с учетом свойства антиципации, если того требует быстрое изменение внешних условий.

В качестве профилактики несчастных случаев и ЧП при выявлении

неуравновешенности эмоциональных процессов предлагается использовать самовоспитание и методы, позволяющие выработать у индивида самообладание.

Во втором случае профилактической мерой является тщательное наблюдение за деятельностью таких людей и ограничение допуска к работам, в которых защищенность обеспечивается главным образом за счет способности к моментальной реакции, быстрым и точным действиям.

Пагубные пристрастия к алкоголю, наркотикам отрицательно влияют на все сферы психического состояния человека.

Рассматривая алкогольную астению (похмелье), можно отметить, что практически у каждого здорового человека в организме содержится от 0,2 до 0,3 ‰ (промиля) алкоголя. Много это или мало? Уже 0,5 ‰ изменяет психическое состояние человека. А только кружка пива дает повышение алкоголя в крови человека до 0,8 ‰. Медики констатируют, что каждый прием алкоголя убивает 100 тыс. мозговых клеток. При частом приеме алкоголя и в больших количествах наступает деградация личности.

С позиций безопасности в сфере экономической деятельности (коммерческой, предпринимательской, банковской и др.) особое значение имеет послеалкогольная астения. Развиваясь в дни после употребления алкоголя, она не только снижает работоспособность человека, но и ведет к заторможенности и снижению чувства осторожности (по русской пословице – пьяному и море по колено).

Длительное употребление алкоголя вызывает алкоголизм – болезненное привыкание к алкоголю, сопровождающееся различной степенью деградации личности. Специалисты, страдающие алкоголизмом, утрачивают свойственную им точность и аккуратность в работе. Они все чаще допускают ошибки и становятся неспособными к решению сложных творческих задач, к быстрой и правильной ориентации в экстремальных производственных ситуациях.

Изменчивость психической деятельности под влиянием бытовых и производственных воздействий ставит перед инженерами-организаторами экономической деятельности задачу создания и совершенствования систем контроля психического состояния работника в сфере коммерции, предпринимательства и др.

Неудовлетворенность работой и отсутствие интереса к ней. Человек, не интересующийся своей работой и не получающий от нее удовлетворения, не способен психологически правильно настроиться и сосредоточить свое внимание на точном выполнении приемов и движений. Его поведение характеризуется как неуверенное, а внимание – рассеянное. Именно такие отклонения в поведении человека являются чаще всего причиной несчастного случая и ЧС. Вот почему с точки зрения безопасности необходимо, чтобы работник выбрал род занятий, отвечающий его интересам и наклонностям. Кстати, это хорошо сочетается со ст. 18 Конституции РФ.[42]

Однако неудовлетворенность может формироваться и взаимоотношением работника с трудовым коллективом. В этом случае необходимо в коллективе создать такую обстановку, которая бы благоприятно воздействовала на тех работников, кто не проявляет должного внимания к своей деятельности, заинтересованности к успехам и традициям коллектива. Соответствующее отношение коллег по работе, руководителей может изменить первоначальное отношение работника к своей деятельности, может способствовать тому, что он «прикипит» сердцем к своей работе. И, наоборот, отрицательное отношение в конце концов может отбить всякий интерес к работе и желание трудиться. А человек, выполняющий равнодушно свою работу, не любящий ее, как правило, выбирает такую форму поведения, которая закономерно ведет к несчастному случаю или ЧП. Если же у человека складываются положительные эмоциональные отношения к своей работе и рабочему месту, то даже при относительно небольшом интересе он может усвоить формы поведения, повышающие его защищенность и обеспечивающие безопасность его деятельности.

Шантаж и угроза. Человек, который подвергается шантажу или угрозе, находится под гнетом постоянного психического напряжения. Как правило, человек, находящийся длительное время в подавленном психическом состоянии, не способен правильно оценивать обстановку, происходящие события, свое место в коллективе, теряет контроль над своими действиями и допускает в них просчеты. В конечном итоге эти просчеты могут способствовать возникновению различного рода негатив-

[42] Конституция Российской Федерации

ных происшествий не только с ним, но и коллегами по работе, членами его семьи.

7.3.2. Факторы, временно повышающие подверженность риску

Наряду с факторами, устойчиво повышающими подверженность человека риску, имеются также такие факторы, которые или появляются лишь в определенный период трудового процесса, или влияют на поведение работника в течение короткого времени, исчисляемого несколькими часами или даже минутами. К таким факторам можно отнести:

- Неопытность.
- Неосторожность и осторожность.
- Утомление.

Неопытность. Практический опыт является фактором, снижающим подверженность опасности несчастного случая и ЧП. Профессионализм, стаж работы человека влияют на повышение его безопасности.

Одной из предпосылок безопасной работы является выработка известных навыков и сноровки в трудовом процессе. Эти качества влияют на все поведение работника на рабочем месте и отражаются в темпе, ритме, интенсивности работы и, как следствие, повышении производительности трудового процесса и качестве выполняемых работ. К тому же эти качества позволяют работнику высокой квалификации в силу лучшего знания всех сторон производственного процесса быстро ориентироваться, если в работе возникают какие-либо сбои, вызванные негативными ситуациями. Эти качества формируют у него уверенность в себе и коллегах, что также способствует повышению его защищенности и снижению вероятности возникновения несчастного случая или ЧП.

В свою очередь, уверенно чувствуя себя в производственной обстановке, человек быстрее приспосабливается к неблагоприятным воздействиям производственной среды (шум, монотонность работы и др.) и более быстро приобретает опыт. Приобретенный работником опыт позволяет ему правильно распределить свое внимание в соответствии с требованиями технологического регламента или соответствующими указаниями. А это, в свою очередь, позволяет ему правильно нагрузить нервную систему, давая ей соответствующий периодический отдых. Правильное управление вниманием одновременно приводит и к уменьшению энер-

готрат, и отдалению наступления усталости и, как следствие, к повышению его защищенности и безопасности. Практический опыт играет активную роль и в выработке автоматизма поступков.

С одной стороны, практика закрепляет навыки, так как уменьшает участие второй сигнальной системы человека и необходимость волевого вмешательства при выполнении рабочих приемов и операций.

С другой стороны, выработанный автоматизм как бы сковывает рабочего: он жестко привязан к точному выполнению ранее заученных движений. По мере дальнейшего закрепления автоматизма работник выполняет работу гораздо свободнее, может позволить себе ввести в нее некоторые изменения, как бы варьируя приемами. В подобных случаях сознание вмешивается в управление деятельностью время от времени. Это означает, во-первых, известную степень отключения, от чего он начинает выполнять работу более заинтересованно. Во-вторых, это оберегает его от полного отключения мыслей от управления работой, а стало быть, и благотворно влияет на концентрацию внимания.

Причину повышения подверженности риску под влиянием неопытности необходимо искать, в первую очередь, в том, что работник еще не научился приспосабливаться ко всем требованиям, которые предъявляет ему работа. Отрицательное воздействие неопытности проявляется по нескольким причинам, которые могут привести к несчастному случаю или ЧП:

- в результате недостаточно выработанных навыков значительно возрастает вероятность всякого рода ошибок на рабочем месте,
- вследствие ожидания того, что могут произойти эти ошибки. Такое ожидание оказывает отрицательное влияние вследствие чрезмерной концентрации внимания на выполнение правильных движений, что, в свою очередь, приводит к быстрому утомлению, в результате которого теряется внимание,
- из-за формирующегося у человека психического состояния тревоги, замешательства, ощущения неуверенности в своих действиях. Все это может вызвать ошибки в непосредственном управлении движениями, особенно в тех случаях, когда движения требуют очень тонкой координации со стороны ЦНС,
- в связи с желанием человека подавить в себе чувство неуве-

ренности, самоутвердиться перед коллегами, как бы бравируя своим отношением к опасности, тем самым становится более склонным к ней.

- из-за еще невыработанной в себе трудовой дисциплины, в том числе и пренебрежения к требованиям безопасности.

Надо иметь в виду, что степень опытности не определяется стажем работы по специальности. Фактический уровень опытности зависит от таких факторов, как сноровка, навыки, приобретенные в процессе обучения, особенности личности (заинтересованность, способность мышления, ловкость движений и т.д.) и, наконец, характер влияния производственного коллектива на работника и его поведение, характеризующий выработку и закрепление основных с точки зрения безопасности навыков и привычек. Например, в коллективе, в котором требования безопасности выполняются всеми работниками без исключения, новичок более быстро освоит и закрепит необходимые требования безопасности. И, наоборот, в коллективе, в котором к требованиям безопасности относятся с пренебрежением, «спустя рукава», новичок не приобретет достаточных навыков и не закрепит их даже при длительной работе в таком коллективе.

Это дает возможность заключить, что навыки безопасности должны составлять органическое единство с другими навыками трудовой деятельности и рассматриваться как составной элемент этой деятельности. Одновременно навыки не должны формировать у рабочих чувство обремененности дополнительными действиями, необходимыми для обеспечения безопасности.

Неосторожность. Она выступает одним из факторов, увеличивающим подверженность опасности одного работника или целого коллектива в течение какого-то неопределенного времени.

Неосторожность – это такой фактор, который увеличивает подверженность опасности одного работника или целого коллектива в течение какого-то времени.[43]

Осторожность является противоположным фактором. Однако нельзя отождествлять осторожность и неуверенность.

Осторожность, вырабатывающаяся на основе профессионального знания дела, проявляется именно в том, что рабочий:

---

[43] Балинт И., Мурани М. Психология. Безопасность труда. - М.: Профиздат, 1998. - 207 с.

- приобретает способность заранее определить, какие последствия влечет за собой использование неисправного оборудования, приспособлений, орудий труда и невыполнение технологического регламента или предписаний,

- требует своевременного проведения необходимых регламентных работ на оборудовании, приспособлениях, орудиях труда, средствах контроля ОВПФ и параметров окружающей обстановки,

- соблюдает самостоятельно порядок на рабочем месте, следит за тем, чтобы своевременно удалялись побочные продукты, готовые изделия и отходы технологического процесса.

Существенное различие состоит в том, что боязливый человек осмотрителен, так как он еще не овладел определенными навыками, необходимыми для безопасной работы, и осознает это.

Осмотрительность осторожного человека основана на хорошем знании условий своей деятельности, спокойном отношении к опасности, отработанном до совершенства автоматизмом действий и сознательном постоянном контроле над этими действиями.

Способность человека к осторожности, осмотрительности проявляется чаще всего в таких формах, как:

- Рациональное управление своим вниманием.
- Правильное использование доведенных да автоматизма действий.
- Дисциплинированность.
- Поддержание порядка на рабочем месте.

Рациональное управление своим вниманием. Осторожный человек всегда знает, когда сосредоточить свое внимание на трудовом процессе, а когда можно позволить немного отвлечься. Для осторожного человека характерна внутренняя сосредоточенность, с помощью которой он оберегает себя от воздействия внешнего мира, не позволяет нарушить необходимый внутренний настрой на работу и, конечно, сам не отвлекает своих коллег.

Умение правильно распределить внимание выражается в том, что колебания степени концентрации внимания сознательно подчиняются объективным требованиям трудового процесса.

Правильное использование выработанного автоматизма действий. Работник знает, когда необходим сознательный контроль действий,

доведенных до автоматизма, а когда он может полностью положиться на выработанные в результате обучения и практики навыки. Правильно чередуя автоматическое выполнение операций с деятельностью, осуществляемой под контролем мышления, опытный работник, во-первых, облегчает свой труд, а во-вторых, делает его более содержательным.

Дисциплинированность. Она проявляется в аккуратном и точном выполнении требований технологического регламента или определенных должностных и технологических инструкций, своевременном использовании предназначенных средств защиты. При неосторожности характерно пренебрежительное отношение к выполнению требований и предписаний, а также к использованию необходимых средств защиты. Из-за упушений в этой области происходят многочисленные несчастные случаи, ЧП и профессиональные болезни.

Поддержание порядка на рабочем месте. Осторожный, дисциплинированный работник не поленится перед началом работы проверить оборудование, приспособления и орудия труда для того, чтобы избежать повышенного риска в процессе своей деятельности.

Утомление работника играет ведущую роль в возникновении отрицательных явлений, которые подавляют его интерес к выполняемой работе, снижают его работоспособность, влияют на качество самой работы. С точки зрения подверженности несчастному случаю и ЧП утомление является весьма значимым фактором.

Рассматривая утомление, следует различать, с одной стороны, утомление, которое характеризуется существенными сдвигами физиологических функций, с другой стороны, ощущение усталости как условие предупреждения утомления, которое периодически ощущается каждым работающим в процессе трудовой деятельности.

Состояние утомления является следствием различных нарушений в организме, отклонений от нормы в функциях нервной системы. В особо тяжелых случаях утомление может рассматриваться как патологическое явление, повышающее подверженность факторам риска.

Переутомления можно избежать за счет своевременного отдыха или даже лечения, а также за счет перевода на другую менее напряженную работу.

Как один из факторов, снижающих переутомление, можно рассмат-

ривать деятельность в соответствии с правильной динамикой работоспособности, характеризующейся следующими циклами:

- периодом врабатываемости, который может длиться от 15 минут до 2,5 часов,
- фазой устойчивой работоспособности, продолжительность которой может составлять от двух до четырех часов,
- периодом снижения работоспособности.

Рабочий процесс утомляет, естественно, не только слабого человека, но и человека с нормальной выносливостью. Это связано с тем, что вслед за усталостью в центральной нервной системе человека появляются различные процессы, которые воздействуют непосредственно на его психическую деятельность, снижают защищенность от опасности.

Утомление возникает в результате сложных, полностью не выясненных физиологических процессов. Обычно различают физиологическое и психическое утомление.

Физиологическое утомление выражает, прежде всего, воздействие на нервную систему продуктов разложения, освобождающихся в результате мускульной деятельности.

Психическое утомление возникает в результате перегруженности самой ЦНС человека.

Как правило, в большинстве рабочих процессов участвуют одновременно определенные группы мышц, формирующих мускульную деятельность и нервы. Таким образом, явления этих двух видов утомления взаимно переплетаются.

В результате утомления наступает состояние усталости, которое само по себе исключительно неустойчивое, текучее и степень которого не находится в прямой зависимости от содержания или интенсивности трудовой деятельности. В силу этого получается, что психическое утомление, т.е. появление усталости, обычно предшествует утомлению физиологическому. Чувство усталости в психическом смысле в первую очередь проявляется в эмоциональной области (безразличие, скука, состояние излишней напряженности и т.д.).

По мере углубления состояния утомления во всех областях психической жизни наступают изменения, отрицательно воздействующие на

дееспособность работника и, главным образом, затрудняющие точное, согласованное выполнение работы. Психическое утомление обнаруживается в следующих явлениях:

- в области ощущений,
- снижается способность концентрации внимания,
- уменьшается способность к запоминанию,
- падает помехоустойчивость ЦНС.

В *области ощущений* психическое утомление выражается в понижении восприимчивости работником различных раздражающих факторов, в результате чего отдельные их раздражения он вообще не воспринимает, а другие воспринимает лишь с опозданием.

В случае *снижения способности концентрировать внимание* возникает неравномерность в степени напряженности внимания, возможность сознательного его регулирования уменьшается, а затем внимание и вовсе исчезает. Одновременно с этим усиливается непроизвольное внимание под воздействием внешних факторов, отвлекающих работника от трудового процесса.

При *уменьшении способности к запоминанию* становится труднее вспоминать уже известные вещи, причем воспоминания становятся обрывочными. Такого рода временное нарушение памяти не позволяет работнику в случае возникновения неожиданных перебоев в работе оборудования или других неисправностей в рабочем процессе с должной скоростью применять свои профессиональные знания для их устранения. Человек не может действовать с упреждением, так как отсутствует чувство антиципации.

Мышление уставшего человека становится замедленным, неточным. Оно в какой-то мере теряет свой критический характер, гибкость, широту.

В области эмоциональной жизни под влиянием утомления могут возникнуть явления депрессии или повышенной раздражительности, наступает эмоциональная неустойчивость.

Помехи для деятельности нервных функций, обеспечивающих сенсорную координацию, а также для сложнейших функций самих двигательных центров, позволяющих выполнять особо значимые и координированные движения, способствуют потере скорости и точности движений, что приводит к быстрому росту усталости. В результате этого

время реакции усталого человека увеличивается, а следовательно, он медленнее реагирует на внешние воздействия и одновременно на какой-то период даже теряет ловкость.

В результате утомления в течение какого-то периода времени наблюдаются характерные колебания не только в степени интенсивности работы, но и в психическом состоянии работника. Вот почему контроль периодичности таких колебаний имеет большое значение для безопасности трудовой деятельности.

Исследования медиков показывают, что явления утомления в утренней смене интенсивнес всего наблюдаются на четвертом и пятом часу работы. В вечерней и ночной смене – уже в самом начале смены, после чего этот процесс затухает, а в середине смены проявляется вновь, и затем после относительного уменьшения вновь усиливается в последние часы работы. Момент наступления кульминационных периодов и их продолжительность зависят от характера работы, условий труда и физического развития работника. Эти кульминационные периоды являются физиологическими критическими точками трудовой деятельности. Как раз в эти периоды можно наблюдать наиболее выраженные изменения в физических функциях, и именно в эти отрезки времени происходит большинство несчастных случаев и ЧП.

Нельзя правильно судить об этой периодичности в процессе утомления, если не учитывать при этом нагрузку человека в нерабочее время.

Остаточное утомление человека в процессе деятельности перед ее началом затрудняет процесс его приспособления к условиям работы и временно усиливает степень риска получения травмы или происшествия чрезвычайного события.

Профилактикой снижения утомления является снижение монотонности, так как ощущение усталости возникает с чувством скуки, вызываемого монотонностью. Например, развитие процесса утомления можно замедлить, если предусмотреть короткие паузы в процессе работы; они будут особенно эффективны, если человек заполнит эти паузы активным отдыхом.

Однако отрицательное влияние утомления на безопасность трудовой деятельности нельзя устранить только мерами по улучшению условий

труда на рабочем месте. Необходимо правильно организовывать и образ жизни работников. Очень важно, чтобы перед началом работы трудящиеся не утомляли себя другими видами деятельности. Необходимо создавать условия для соблюдения ими нормальной продолжительности сна (7-8 ч. ежедневно) и питания. Они должны вести здоровый образ жизни.

7.4 Психические состояния, возникающие в результате чрезвычайных воздействий опасных факторов

В предыдущем разделе отмечалось, что влияние утомления обнаруживается периодически, что усталость временно повышает подверженность опасности. Эти периодические колебания в значительной степени усиливаются, если человек приступает к работе после предшествующей нагрузки или значительного стресса (бессонная ночь, семейные неурядицы, плохое самочувствие). В таких случаях остаточное утомление воздействует уже как чрезвычайный фактор на его индивидуальную деятельность, повышает его подверженность риску.

Подверженность опасности увеличивается еще в большей степени, если повышенная усталость работника сочетается с тревожным, беспокойным психическим состоянием (трагическое событие, сильный стресс при следовании на работу и др.). Сильные эмоциональные переживания могут стать существенным фактором возникновения несчастного случая и ЧП на производстве, в пути следования на личном транспорте. Опасность таких переживаний заключается еще и в том, что эмоциональная неуравновешенность может продолжаться несколько дней, что отрицательно сказывается на таких психических процессах, как внимание.

Временные нарушения функции внимания могут проявиться в изменении общего настроения, например рассеянности, вызвать нарушение координации движений и, как следствие, привести к проявлению разного рода ошибок.

Усилить подверженность риску может и состояние так называемой психической атмосферы в коллективе из-за конфликтных ситуаций перед работой или непосредственно на рабочем месте. Особо сильно этот чрезвычайный фактор может проявиться в женском коммерческом кол-

лективе, так как женщины более подвержены эмоциональным воздействиям.

Однако следует обратить внимание на то, что потеря внимания может произойти и в результате, казалось бы, положительных эмоций (например, неожиданно возникшей сильной радости, проявления сильного эмоционального чувства) или состояния напряженного ожидания какого-либо события.

Интенсивное внешнее раздражение наряду с отвлечением внимания и в связи с ним часто вызывает нарушение динамического стереотипа человека, что приводит к временному сбою в работе или неверным движениям и изменению координации. Если эти явления проявятся на той фазе рабочего процесса, когда точность движения особенно необходима для обеспечения безопасности, то они повысят вероятность возникновения несчастного случая или ЧП.

Таким образом, психические состояния, возникающие вследствие исключительных воздействий, повышают индивидуальную подверженность опасности по двум причинам:

- работник становится временно неосторожным из-за подобного психического состояния,
- его внимание становится менее устойчивым, утрачивается уверенность в движениях.

Различные отклонения подобного рода нередко проявляются в сочетании друг с другом и могут значительно повлиять на индивидуальную защищенность работника в трудовом процессе.

7.5 Роль некоторых особо важных факторов в обеспечении безопасности

Для того чтобы найти решения, направленные на повышение защищенности человека, в том числе и в экстремальных ситуациях, и сокращение числа несчастных случаев и ЧП на производстве необходимо сформулировать некоторые конкретные задачи в области безопасности жизнедеятельности и выделить роль отдельных вещественных и субъективных факторов в обеспечении безопасности в экономической сфере деятельности.

7.5.1 Роль вещественных факторов в предупреждении и предотвращении несчастных случаев и чрезвычайных происшествий

Предупреждение и предотвращение несчастных случаев и ЧП, вызванных воздействием внешней среды, представляют техническую сторону безопасности жизнедеятельности и, в частности, экономической безопасности в производственной деятельности.

Поэтому это относится к прерогативе техники безопасности, как одной из составных частей охраны труда, и не определяется психологией безопасности.

Однако следует кратко привести несколько таких, частью общих, а частью специфически психологических аспектов, которые имеют значение для предотвращения несчастных случаев и ЧП в коммерческой деятельности.

К таким жизненно важным задачам относятся:

- Определение степени опасности несчастного случая или ЧП (степени риска).
- Выбор и проведение соответствующих мероприятий, устраняющих феномен опасности или снижающих фактор риска.
- Учет требований безопасности при обеспечении рабочего места в сфере экономической деятельности. Такой учет дает возможность обеспечить соответствующей безопасной техникой, необходимым в соответствии с факторами риска защитным оборудованием, организовать производственные процессы с точки зрения безопасности, в том числе и экологической.
- Метрологическое обеспечение и контроль ОВПФ, средств коллективной и индивидуальной защиты на каждом РМ.
- Постоянный контроль РМ на соответствие нормативным условиям труда и требованиям научной организации труда.

7.5.1.1 Определение степени опасности возникновения несчастного случая или чрезвычайного происшествия

Определить степень опасности несчастного случая или ЧП (степень риска) можно в следующей последовательности:

1. Выяснить как можно точнее и обстоятельнее, на каких рабочих

процессах, даже на каких этапах и операциях этих процессов, возможно воздействие на работника ОВПФ. На каком этапе работы работник подвержен максимальной опасности, которая может привести к несчастному случаю или ЧП. Это можно выполнить после:

- изучения вида и типа ошибок, которые в действиях работающих могут обусловить возможность возникновения несчастного случая и ЧП на каждом из рабочих мест,
- вскрытия тех моментов психофизиологического управления деятельностью, которые играют существенную роль в динамике работоспособности личности с учетом специфики трудовых движений, требований технологического регламента или соответствующей инструкции или предписания и ритма жизнедеятельности человека. В свою очередь, это требует определения, какие специфические требования предъявляют работнику каждая сфера деятельности и каждый вид работы.

В результате такого анализа можно значительно повысить эффективность использования мер безопасности как в профессионально-техническом образовании (расширение сферы информационной безопасности), так и в обучении работников правилам безопасности, в повышении их знаний в области безопасности жизнедеятельности (профилактика безопасности и расширение сферы защищенности).

2. Выяснить все мешающие работнику факторы не только непосредственно трудового процесса на РМ, но и факторы производственной среды (например, параметров микроклимата, акустической загрязненности, выделения вредных веществ и т.п.), а также возможности использования психологического воздействия для уменьшения влияния этих факторов (увеличение сферы психологической защищенности).

Выбор и проведение мероприятий. При проведении мероприятий, направленных на устранение опасности (риска), вызванных воздействием вещественной среды, необходимо:

- Стремиться к совершенствованию защитного оборудования с учетом не только источников риска, но и субъективных факторов, которые могут играть существенную роль в определении положительного или отрицательного отношения работника к использованию защитных средств. Надо считаться с тем, что эффективность средств защиты не определяется только их защитными свойствами, но и зависит от быст-

рой приспособляемости к этим средствам работников. Эти средства защиты не должны стать обузой для них и излишне их обременять.

- Добиваться эффективности мер безопасности за счет факторов, вызывающих возбуждение внимания, направленного на информационную совместимость рабочего в системе «человек-машина». Например, использовать соответствующие цветовые сигналы и текстовые предупреждения на всех рабочих местах, где существует высокая вероятность несчастного случая или ЧП.

Учет требований безопасности при приобретении и установке оборудования, организации безопасных производственных процессов. Аспекты безопасности труда необходимо учитывать на всех стадиях жизненного цикла функционирования коммерческой или предпринимательской организации – от проектной разработки, строительства, приобретения и установки оборудования, защитных средств, организации безопасных производственных процессов до ликвидации коммерческой или предпринимательской структуры. В этой связи большое значение для обеспечения безопасности приобретают следующие действия:

- Покупая оборудование, следует обратить внимание на его узлы и части, за которыми работник постоянно наблюдает в процессе трудовой деятельности. Эти узлы и механизмы должны обязательно выделяться по цвету на фоне всей конструкции и располагаться в поле зрения работающего.
- Оборудование для безопасного выполнения техпроцесса должно выбираться в соответствии с эргономическими требованиями и учитывать рабочую позу работника.
- Рабочее место должно соответствовать требованиям эргономики – исключать неудобную рабочую позу, при которой легко может возникнуть неуверенность движений, нарушение равновесия, неточность координации движений и т.д.

Метрологическое обеспечение и контроль ОВПФ. При организации экономической деятельности необходимо правильно применять средства контроля безопасности оборудования, приспособлений, орудий труда, инструмента, коллективных и индивидуальных средств защиты с учетом требований метрологии и средства оповещения работников о нарушении режимов ведения технологического регламента или выходе параметров

факторов за допустимые значения. Это диктуется тем, что при наступлении критической ситуации работник должен своевременно получить информацию о возможной аварии, чтобы быть готовым к правильным действиям по ликвидации причин возникновения несчастных случаев, ЧП.

Постоянный контроль рабочего места на соответствие требованиям условий и научной организации труда. Проведение постоянного контроля рабочего места на соответствие требованиям условий и научной организации труда вытекает из условий безопасности работника на своем рабочем месте. Захламленность рабочего места может стать дополнительным источником опасности для работника. Все параметры, характеризующие производственную среду, должны отвечать требованиям производственной санитарии.

7.5.2 Роль субъективных факторов в предупреждении и предотвращении несчастных случаев и чрезвычайных происшествий

Прежде чем рассматривать роль субъективных факторов в предупреждении и предотвращении несчастных случаев и ЧП, необходимо хотя бы кратко сформулировать те важные с психологической стороны требования, которые должны предъявляться к субъективным факторам безопасности труда в коммерческих или предпринимательских организациях. Эти требования органически переплетаются с теми требованиями, которые предъявляются вообще работникам, таким как: выработка способностей и навыков, необходимых для умения приспособиться к объективным условиям среды, а также нормы поведения и мотивы поступков, являющиеся предпосылкой повсдения. Наиболее существенные задачи в этом направлении следующие:

- Учет особенности нервной системы каждого работника.
- Обучение профессионализму и наработке соответствующих форм поведения, требуемых в соответствии с создаваемой ситуацией.
- Обеспечение защищенности от факторов риска.
- Организация постоянного контроля соблюдения требований, правил и норм безопасности.

Учет особенности нервной системы каждого работника. Особенность нервной системы каждого человека должна учитываться с целью

правильного анализа индивидуальных качеств и условий труда на рабочем месте по степени риска. Эта задача очень сложная и требует от распределителя работ умения правильно расставить работников в зависимости от их индивидуальных качеств: ловкости, умения быстро ориентироваться и действовать в критической ситуации, способности к концентрации внимания и т.д. Чаще всего распределитель работ полагается на свои опыт и интуицию, которые порой не позволяют достаточно точно и достоверно определить необходимые качества работника в той или иной сфере экономической деятельности.

Не случайно поэтому в последнее время для точного установления профессиональной подверженности фактору риска проводятся тщательные испытания на пригодность для особо опасных и значимых видов работ. С помощью таких испытаний устанавливается, кто из работников подходит к повышенной опасной сфере деятельности и кого нецелесообразно привлекать в связи с высокой степенью опасности.

Организация испытаний на пригодность, естественно, предполагает тщательный анализ трудовых процессов с учетом вещественных факторов:

- Критических точек на всех фазах трудовой деятельности, т.е. тех операций или таких отрезков времени, когда работник больше всего подвержен воздействию факторов риска или когда ошибки в действиях с наибольшей вероятностью приводят к аварии, несчастным случаям или ЧП.
- Нарушение каких именно психических функций чаще всего вызывают несчастные случаи или ЧП в сфере каждого рода трудовой деятельности? Например, отвлечение внимания, потеря бдительности и т.п.

Такой тщательный анализ позволяет разработать конкретную методику испытаний (тестирования) работников с целью достоверного установления тех качеств и характерных особенностей, которыми непременно должен обладать каждый в рассматриваемой сфере деятельности. Кроме того, методика позволяет выявить, интересуется ли работник той сферой деятельности, которую он профессионально выбирает, может ли у него выработаться положительное отношение именно к выбираемой сфере деятельности.

Испытания (тестирование) рекомендуется проводить в возможно ран-

нем трудовом возрасте: до обучения специальности или поступления на работу, так как подверженность фактору риска в наибольшей степени встречается у начинающих трудовую деятельность.

Поэтому самый действенный метод предупреждения несчастного случая и ЧП – это воспрепятствование поступлению на работу с повышенной опасностью таких лиц, подверженность которых факторам риска еще больше возрастает из-за их психологической непригодности.

Обучение профессионализму и наработке соответствующих форм поведения, требуемых в соответствии с создаваемой ситуацией. Пригодность сама по себе еще не гарантирует сокращение подверженности факторам риска. Исключительную роль играют профессиональные знания и выработка форм поведения, необходимых для приспособления к опасности и «расширения» сферы защищенности личности.

Защищенность от фактора риска. Защищенность, сформировавшуюся в процессе обучения и практики, необходимо постоянно подкреплять (тренировать), т.е. вновь и вновь напоминать работникам об опасности, наличии факторов риска и мерах их предупреждения, на что и направлены, как правило, инструктажи с работниками, а также инструкции по каждому виду профессий и деятельности.

Постоянный контроль соблюдения требований, правил и норм безопасности. Кроме обучения и разъяснительной работы, следует постоянно контролировать соблюдение нормативных актов, правил и норм предупреждения и предотвращения несчастных случаев и ЧП, выполнение мер безопасности. Важной мерой предупреждения и предотвращения несчастных случаев и ЧП является своевременное выявление нарушителей требований безопасности и привлечение виновных к ответственности в соответствии с допущенным нарушением правил и норм.

Глава 8. УСТОЙЧИВОСТЬ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ ЭКОНОМИКИ

8.1 Техногенные катастрофы и их роль в разрушении экономики

8.1.1 Технологические аварии как источники техногенных катастроф

Источник риска характеризуется высвобождением энергии в процессе функционирования самого источника, концентрацией энергии по месту действия и времени и постепенным накоплением факторов риска, параметры которых отличаются по величине и интенсивности от расчетных или допустимых значений, а также факторов, вызванных неправильными или несвоевременными действиями персонала.

К источникам риска можно отнести:

- предприятия и производства,
- технологические процессы, в которых предусматривают использование высоких давлений, температур, взрывчатых, легковоспламеняющихся, а также химически агрессивных, токсичных, биологически активных и радиационно-опасных веществ и материалов,
- продукция и отходы,
- гидротехнические сооружения,
- транспортные средства,
- продуктопроводы,
- места захоронения отходов токсичных и радиоактивных веществ,
- здания и сооружения, построенные с нарушением строительных норм и правил (СНиП),

- военная деятельность,
- терроризм и т. п.

Обычно накопление каких-либо факторов риска (дефектов в оборудовании, отклонений от установленных документацией процедур ведения процесса) инициирует со временем их действие, создающее аварийную ситуацию или приводящее к угрозе возникновения промышленной аварии.

Промышленная авария чаще всего выражается экстремальным событием техногенного происхождения. Она же может характеризоваться цепью событий, являющихся следствием случайных внешних воздействий, которые приводят к выходу из строя, повреждению и (или) разрушению технических устройств, транспортных средств, зданий, сооружений, а также человеческим жертвам. Аварии технических систем предшествуют техногенным катастрофам, увеличивающим техногенный риск для объектов экономики и экономических систем в целом. К технологическим авариям и связанным с ними техногенным катастрофам обычно относят аварии на энергетических, химических, биохимических объектах, транспортных коммуникациях, при перевозке разрядных грузов, на продуктопроводах и т. д.

Производственная авария является частным случаем аварии, приводящей к техногенным катастрофам из-за нарушения технологического регламента. К техногенным катастрофам технологического характера могут приводить и изменение фоновых значений различных природных сред (атмосферы, гидросферы, литосферы), а в некоторых случаях и таких характеристик Природы, как климата Земли, озонового слоя планеты, условий освещенности и других природных систем за счет фонового техногенного загрязнения, формирующегося в основном под влиянием промышленных выбросов, а также условий регионального и глобального распределения этих загрязнений.

Ущерб от техногенных катастроф определяется как прямыми, так и косвенными потерями, наносящими существенный сбой нормальному функционированию экономики любого государства.

Примером прямых потерь в СССР можно назвать потери от Чернобыльской аварии в виде разрушения 4-го блока атомной электростанции (АЭС).

Косвенные потери: города на подтопленных территориях, загубленный чернозем, засоленные орошением почвы, истощенные загрязненные горизонты артезианских вод, Азов и Арал, разбуженная вечная мерзлота, вода и воздух, исчезнувшие растения и животные и, главное – здоровье человека, детская смертность, нарастающий генетический груз затяжного техногенного кризиса, обусловленного серьезным загрязнением окружающей среды и подрывом природно-ресурсного потенциала государства.

В первую очередь возрастает риск аварий крупных технологических систем, что связано с увеличением их числа и сложности, ростом единичной мощности агрегатов на промышленных и энергетических объектах, их территориальной концентрацией.

По далеко не полным данным, охватывающим только крупнейшие промышленные катастрофы прошедшего столетия, более половины из них разразились в течение последних двух его десятилетий. Множество катастроф произошло в различных странах и в начале этого столетия. Возросла угроза возникновения техногенных катастроф и в связи с обострившимся в различных странах терроризмом. Это связано с тем, что разрушительный потенциал крупных технологических катастроф в настоящее время сопоставим с угрозой военно-политических ЧС. Только в сфере энергетики добывается, хранится и перерабатывается около 10 млрд тонн условного топлива – масса, способная гореть и взрываться, сравнимая с арсеналом ядерного оружия, накопленного в мире за всю историю существования человечества. Сопоставима и разрушительная сила некоторых технологических катастроф в военных операциях. Так, совокупная численность убитых и раненых в результате атомной бомбардировки Нагасаки в 1945 г. составила около 140 тыс. человек. Вследствие утечки ядовитого газа на химическом заводе в Бхопале (Индия) в 1984 г. погибли свыше 220 тыс. человек.

Важным фактором масштабности промышленной катастрофы является концентрация производств на небольшом пространстве и взаимовлияние таких производств друг на друга. Например, рассматривая последствия от размещения рядом АЭС и тепловой электростанции (ТЭС), использующей органическое топливо, можно выделить следующие фак-

торы взаимовлияния. Известно, что АЭС большой мощности являются причиной повышения влажности воздуха на значительных расстояниях от места своего расположения. В то же время ТЭС представляет собой источник выбросов SO_2, попадание которых в атмосферу с повышенной влажностью способствует образованию в ней увеличенной концентрации серной кислоты. Она представляет серьезную угрозу стабильному функционированию сельского хозяйства, экологическим системам и населению в ареале распространения этих факторов, т.е. ведет к экономическим потерям и представляет угрозу экономике государства.

В самом общем случае авария на одном предприятии, вызывающая аварию на рядом расположенном объекте, может вызвать аварию на следующем экономическом объекте.

8.1.2 Последствия аварий и техногенных катастроф и преднамеренного (в военных целях) воздействия на объекты экономики

Любая крупная техногенная авария влечет за собой возникновение ЧС, грозящих дестабилизацией или разрушением не только социальных и экологических систем, но и экономических объектов и структур, и потому требуют незамедлительного реагирования со стороны не только правительства, но и всего общества. Такие ЧС могут возникать взрывообразно, вследствие технологических (промышленных, энергетических и т. д.) катастроф, либо «вызревать» подспудно, создавая угрозу близкорасположенному промышленному и другим объектам народного хозяйства. Это так называемый эффект «домино». Такой эффект наиболее опасен при нападении в военное время или в случае терроризма и представляет наибольшую опасность, если в цепочку таких аварий «включится» радиоактивный объект (гражданского или военного назначения). В этом случае разрушение таких объектов может привести экономику любого государства в состояние коллапса из-за развития промышленной катастрофы, приведшей к техногенной ЧС.

Промышленная катастрофа рассматривается как крупная промышленная авария, повлекшая за собой человеческие жертвы, ущерб здоровью людей либо разрушение и уничтожение объектов, материальных

ценностей в значительных размерах, а также приведшая к серьезному ущербу окружающей среды.[44]

Техногенная ЧС характеризуется состоянием, при котором в результате возникновения аварии на источнике технической ЧС на объекте, определенной территории нарушаются нормальные условия жизни и деятельности людей, возникает угроза их жизни и здоровью, наносится ущерб имуществу населения, народному хозяйству и окружающей природной среде.

Источником технической ЧС считается опасное техногенное происшествие, в результате которого на объекте, определенной территории произошла техническая ЧС.

Задачей устранения техногенной ЧС, связанной с технологическими авариями и промышленными катастрофами, следует считать определение соответствующего способа нахождения уязвимости экономической системы и ее объектов и структур при действии факторов риска источников технических ЧС. После определения факторов риска их располагают в определенном порядке в зависимости от относительной уязвимости различных экономических объектов, изменяющей устойчивость экономических объектов в ЧС.

8.2 Понятие об устойчивости объектов хозяйствования в чрезвычайных ситуациях

Под устойчивостью любой технической системы понимается возможность сохранения ее работоспособности при нештатном внешнем воздействии. Согласно этому определению, под устойчивостью работы промышленного объекта понимается его способность выпускать установленные виды продукции в объемах и номенклатуре, предусмотренных соответствующими планами, в условиях чрезвычайных (нештатных) ситуаций, а также приспособленность этого объекта к восстановлению в случае повреждения в кратчайшие сроки.

Для объектов, не связанных с производством материальных ценностей (транспорт, связь, линии электропередач и т. п.), устойчивость определяется их способностью выполнять свои функции. Повышение устой-

[44] ГОСТ Р 22.0.005-94.

чивости технических систем и объектов достигается главным образом за счет проведения соответствующих организационно-технических мероприятий, которым всегда предшествует исследование устойчивости конкретного объекта.

К исследованию устойчивости промышленного объекта обычно привлекается инженерно-технический персонал и работники штаба гражданской обороны (ГО), а в необходимых случаях – научно-исследовательские и проектные организации, связанные с работой исследуемого объекта (принимавшие участие в его проектировании и др.).

Общее руководство исследованиями осуществляет начальник ГО (руководитель предприятия, фирмы), приказом которого определяются сроки проведения работ, состав рабочих групп и планы проведения исследования.

Создаваемые рабочие группы обычно соответствуют основным производственно-техническим службам объекта.

Группа под руководством заместителя директора по капитальному строительству исследует здания основного и вспомогательного производства, транспортные коммуникации объекта, мосты, эстакады, транспортные туннели, подземные переходы и сооружения промышленного объекта.

Группа главного энергетика анализирует условия надежного функционирования коммунально-энергетических сетей, систем водоснабжения и канализации, сетей газо-, электро- и теплоснабжения объекта.

Группа главного механика и группа главного технолога отвечают за безопасное состояние станочного и технологического оборудования, технологических процессов производства.

Бесперебойное управление производством и его материально-техническое снабжение входит в функциональные обязанности групп начальников производства материально-технического снабжения.

В зависимости от особенностей производства на каждом экономическом объекте могут быть выделены дополнительные области исследования и созданы соответствующие группы.

На первом этапе исследования промышленного объекта проводится анализ уязвимости и устойчивости его отдельных элементов в условиях ЧС. Важной частью этой работы является оценка опасности выхода из

строя или разрушения отдельных элементов, а также всего объекта в целом. На этом этапе проводятся работы по анализу:[45]

- последствий аварий отдельных систем производства;
- распространения:
  - ударной волны по территории предприятия (взрыв резервуаров, коммуникаций, взрывоопасных веществ, ядерных зарядов и т. п.),
  - огня при различных видах пожаров;
- надежности установок и промышленных комплексов;
- рассеивания веществ, высвобождающихся при ЧС;
- возможности вторичного образования токсичных, пожаровзрывоопасных смесей и т. п.

При реализации мероприятий по оценке опасности промышленного предприятия (технологической установки) могут применяться различные методы анализа повреждений и дефектов, например метод оценки нарастания повреждения в системе после аварии с построением дерева (схемы) отказов. Для определения возможных аварийных явлений может быть применен метод построения дерева событий, позволяющий корректно использовать информацию о неисправностях компонентов установок и интегрировать ее с данными об окружающих условиях.

На втором этапе разрабатываются мероприятия по повышению устойчивости и заблаговременной подготовке объекта к восстановлению (изменению) после ЧС. Разработанные мероприятия составляют основу плана-графика повышения устойчивости объекта.

В плане или приложениях к нему указываются:

- объем и стоимость планируемых работ,
- источники финансирования,
- основные материалы и их количество,
- машины и механизмы,
- рабочая сила,
- ответственные исполнители,
- сроки выполнения и т. д.

В случае реконструкции объекта в утвержденный план-график вно-

---

[45] Сергеев В.С. Защита населения в чрезвычайных ситуациях. - 3-е изд., перераб. и доп. - М.: Академический Проспект, 2003. - 432 с. - ("Gaudtamus").

сятся изменения и дополнения, порядок принятия которых такой же, как и основного документа.

Исследование устойчивости функционирования объекта начинается задолго до ввода его в эксплуатацию. На стадии проектирования это в той или иной степени делают проектировщики.

Аналогичные исследования объекта проводятся соответствующими службами на стадии технических, экономических, экологических и иных видов экспертиз.

Каждая реконструкция или расширение объекта также требуют нового исследования устойчивости. Таким образом, исследование устойчивости — это не одноразовое действие, а длительный, динамичный процесс, требующий постоянного внимания со стороны руководства, инженерно-технического персонала, служб ГО, министерства чрезвычайных ситуаций (МЧС).

8.2.1 Факторы, влияющие на устойчивость работы объекта

Все промышленные объекты, независимо от их конкретного назначения, имеют много общих черт. Так, любой промышленный объект включает в себя наземные здания и сооружения основного и вспомогательного производства, складские помещения и здания административно-бытового назначения.

В зданиях и сооружениях основного и вспомогательного производства размещаются станочное и технологическое оборудование, сети газо-, тепло-, электро- и прочих видов снабжения. Между собой здания и сооружения соединены сетью внутреннего транспорта, сетью энергоносителей и системами связи и управления.

На территории промышленного объекта могут быть расположены сооружения автономных систем электро- и водоснабжения, а также отдельно стоящие технологические установки и т. д.

Здания и сооружения возводятся по типовым проектам из унифицированных материалов. Проекты производств выполняются по единым нормам технологического проектирования, что приводит к среднему уровню плотности застройки (обычно 30…60%). Все это дает основание считать, что для всех промышленных объектов, независимо от профиля

производства и назначения, характерны общие факторы, влияющие на устойчивость объекта и подготовку его к работе в условиях ЧС.

К общим факторам можно отнести:

- Район расположения объекта.
- Внутреннюю планировку и застройку территории объекта.
- Подготовленность персонала к работе в ЧС и к восстановлению производства.
- Надежность и местоположение жизненно важных систем промышленного объекта (дублирование, ремонтопригодность и т. д.).
- Технологический процесс (особенности используемых веществ; методы обработки, технологический регламент и т. д.);
- Условия эксплуатации зданий, сооружений, опасных технических систем и объектов.
- Надежность и гибкость производственных связей и систем управления производством.

На работоспособность объекта большое влияние оказывает **район его расположения**. Он значительно определяет уровень и вероятность воздействия внешних поражающих факторов природного происхождения (сейсмическое воздействие, сели, оползни, тайфуны, цунами и т. д.). С другой стороны, район расположения может оказаться решающим фактором в обеспечении защиты и работоспособности объекта в случае выхода из строя штатных путей подачи исходного сырья или энергоносителей. Например, наличие реки позволит при разрушении железнодорожных или трубопроводных магистралей осуществить подачу материалов, сырья и комплектующих водным транспортом. Поэтому при исследовании устойчивости работы объекта большое внимание уделяется району расположения объекта. При этом выясняются метеорологические условия территории: количество осадков, направления господствующих ветров, максимальная и минимальная температуры соответственно самого жаркого и самого холодного месяца; по карте изучается рельеф местности, характер грунта, глубина залегания подпочвенных вод, ее химический состав. Проводится анализ:

- топографического расположения объекта,
- характера застройки территории, окружающей объект (структура, тип, плотность застройки),

- уровня опасности смежных производств (гидроузлы, объекты химических производств и т. д.) по минимальному риску,
- естественных условий прилегающей местности (наличие лесных массивов как источников пожаров, водных объектов в виде возможных транспортных коммуникаций, огнепреградительных зон, источников наводнений по условию времени их проявления и т. п.),
- оценки среднегодовых значений ливневых дождей и гроз и т. п.

При изучении **зданий и сооружений объекта** дается характеристика зданиям основного и вспомогательного производства; зданиям, которые не будут участвовать в производстве основной продукции в случае ЧС. Устанавливаются основные особенности их конструкции, указываются технические данные, необходимые для расчетов уязвимости к воздействию ударной волны, светового излучения и возможных вторичных факторов поражения (конструкция, этажность, длина и высота, вид каркаса, стеновые заполнения, световые проемы, кровля, перекрытия, степень износа); оценивается огнестойкость здания. Указывается количество рабочих и служащих, одновременно находящихся в здании (по наибольшей рабочей смене), наличие встроенных в здание и расположенных вблизи убежищ; наличие в зданиях средств эвакуации и пропускная способность.

При оценке **внутренней планировки территории** объекта определяется влияние плотности и типа застройки на возможность возникновения и распространения пожаров, образование завалов входов в убежища и проходов между зданиями. Особое внимание обращается на участки, где могут возникнуть вторичные факторы поражения. На территории объекта такими источниками являются:

– емкости с легковоспламеняющимися жидкостями (ЛВЖ) и ядовитыми сильнодействующими веществами (СДЯВ);

– склады:
- взрывоопасных веществ,
- легковоспламеняющихся материалов,

– взрывоопасные технологические установки;

– технологические коммуникации, разрушение которых может вызвать пожары, взрывы и загазованность участка;

– аммиачные установки и др.

При этом прогнозируются последствия:

- утечки тяжелых и легких газов и токсичных дымов,
- пожаров цистерн, колодцев, фонтанов,
- воздействия молний, в том числе и шаровых,
- взрывов паров ЛВЖ,
- нагрева и испарения бассейнов и емкостей с различными жидкостями, в том числе и СДЯВ,
- рассеивания продуктов сгорания во внутренних помещениях,
- токсичного воздействия на человека продуктов горения и иных химических веществ,
- тепловой радиации при пожарах.

Выполняется оценка возможности образования ударной волны в результате взрывов емкостей, находящихся под давлением, взрывов в закрытых и открытых помещениях и их распространение как внутри, так и снаружи строений. При этом рассматривается суммарный эффект от воздействия динамического и избыточного статического давления в результате ударной волны и проводится оценка количества кинетической энергии и траектории образуемых потоков.

Наряду с этим осуществляются анализ распространения пламени в зданиях и сооружениях объекта, оценка огневого потока в зависимости от расположения стен и внутренней планировки.

Изучается специфика технологического процесса, возможные изменения в нем на время ЧС (изменение технологии, частичное прекращение производства, переключение на производство новой продукции и т. п.).

Группой главного технолога:

Организуется изучение возможностей существующего ТП производства перехода в короткие сроки на новый техпроцесс.

- Оцениваются:
  - возможный новый номенклатурный перечень и возможные сроки перехода на его выпуск;
  - условия хранения готовой продукции, отходов;
  - возможность перехода на ручное управление отдельными элементами технологического оборудования и всем производством в целом:
  - гибкости технологических процессов и возможности замены одних энергоносителей на другие,

- возможности автономной работы отдельных станков, установок технологического процесса (станочных групп, конвейеров, роботов и т. д.) и цехов объекта,
- запасы и места расположения СДЯВ и горючих веществ (ГВ),
- способы и возможности безаварийной остановки производства в условиях ЧС,
- насыщенность производства аппаратурой автоматического управления и контрольно-измерительными приборами.

• Определяется:

- необходимый минимум запасов, который может находиться на территории объекта, и место хранения остальной части в загородной зоне;
- уникальное и особо важное оборудование.

• Дается характеристика станочного и технологического оборудования.

При исследовании **систем** и **источников энергоснабжения**:

• Определяется:

- зависимость работы объекта от внешних источников энергоснабжения;
- необходимые минимальные характеристики энерговооруженности.

• Проводится ревизия энергетических сетей и коммуникаций.

• Анализируются системы автоматического управления и отключения сетей энергоносителей.

При рассмотрении **системы водоснабжения**:

• Обращается внимание на защиту сооружений и водозаборов из подземных источников воды от радиоактивного, химического, бактериологического заражения.

• Определяется:

- надежность функционирования систем пожаротушения;
- возможность переключения систем водоснабжения с соблюдением санитарных правил.

Особое внимание уделяется изучению систем газоснабжения, поскольку разрушение этих систем может привести к появлению вторичных поражающих факторов.

Жесткие требования предъявляются к надежности и безопасности функционирования систем и источников снабжения СДЯВ, сильными окислителями, взрывоопасными и ГВ.

Система управления производством на объекте исследуется на основе изучения состояния пунктов управления и узлов связи, надежности связи с загородной базой, расстановки сил, обеспечения руководства производственной деятельностью объекта во всех подразделениях предприятия в период создавшейся ЧС. Определяются также источники пополнения рабочей силы. Анализируются возможности взаимозаменяемости руководящего состава объекта.

Аналогичным образом проводится исследование других жизненно важных систем предприятия.

8.2.2 Методика оценки устойчивости объекта

Цель оценки устойчивости объекта состоит в выявлении наиболее уязвимых мест в производственных помещениях, сооружениях, технологическом оборудовании и коммуникациях и подготовке предложений по повышению его устойчивости в целом.

Оценка устойчивости объекта проводится в два этапа. В процессе первого на основе прогноза определяют вероятную обстановку, которая может сложиться на объекте при возникновении ЧС. На основе анализа данных, полученных исследовательскими группами, комиссия объекта составляет доклад-справку с приложением соответствующих таблиц и расчетов, в которых перечисляются следующие показатели:

- Характеристика рельефа местности, расположение на ней отраслей объекта, цехов и прогнозирование характера и степени поражения их.
- Оценка:
  - статистической устойчивости к воздействию ударной волны зданий, сооружений, хранилищ, убежищ и пунктов управления техникой и технологическим оборудованием, инженерных коммуникаций.
  - возможной пожароопасной обстановки;
  - радиационной обстановки;
  - возможного воздействия на объект производства вторичных поражающих факторов;
  - зданий и сооружений, которые могут быть использованы для защиты людей;
  - обеспеченности средствами индивидуальной защиты;

• производственных зданий и сооружений, предназначенных для защиты материальных ценностей, продукции, сырья, полуфабрикатов и продовольствия;

• состояния средств связи и оповещения на пункте управления производством.

Справка-доклад обобщается перечнем предлагаемых мероприятий по повышению устойчивости работы объекта.

На втором этапе исследований разрабатывают план мероприятий по повышению устойчивости работы объекта. Этот план является основой деятельности персонала предприятия как в процессе обычного функционирования производства, так и в период угрозы возникновения ЧС. Практическая проверка реальности разработанных мероприятий по обеспечению устойчивости работы осуществляется в ходе специальных или плановых комплексных учений ГО, ЧС на объекте.

Все мероприятия по повышению устойчивости работы объекта являются долговременными. Поэтому часть мероприятий из этого плана включают в хозяйственный годовой план, а другую – в перспективный план развития объекта. В хозяйственные и перспективные планы можно включать только те мероприятия, которые дают отдачу при производстве продукции как в военное, так и в мирное время. Выполнение этих мероприятий должно быть гарантировано выделением финансовых и материальных средств и взято под контроль начальником ГО ЧС и ликвидации последствий аварии объекта.

Оценка инженерной защиты рабочих и служащих объекта. В военное время или террористического нападения защита рабочих и служащих является главной задачей штаба ГО объекта. Для ее выполнения проводится комплекс защитных мероприятий, включающих укрытие людей в убежищах, противорадиационных и других защитных сооружениях, обеспечение средствами индивидуальной защиты и проведение эвакомероприятий. Критерием оценки инженерной защиты служит обеспеченность объекта защитными сооружениями.

Рассматривая вопросы инженерной защиты рабочих и служащих объекта, уточняют положение рассматриваемого объекта по отношению к возможным объектам ядерных ударов. Все возможные объекты, кото-

рые могут подвергнуться ядерному удару, условно делятся на группы, которые:

- расположены в зоне возможных разрушений очага ядерного поражения,
- находятся за границей зоны возможных разрушений, но подвергаются воздействию чрезвычайно опасного, опасного или сильного радиоактивного заражения,
- могут оказаться только под воздействием умеренного радиоактивного заражения или глобальных осадков.

С учетом приведенной классификации в процессе оценки инженерной защиты:

- Изучают:
  - степень обеспеченности работников объекта защитными сооружениями;
  - защитные свойства убежищ, противорадиационных укрытий, жилых, производственных помещений и простейших укрытий должны обеспечивать защищенность людей от основных поражающих факторов ударной волны и радиационного заражения;
  - вместимость каждого защитного сооружения;
  - размеры радиусов сбора;
  - системы жизнеобеспеченности;
  - организацию и надежность оповещения по сигналам ГО.
- Определяют готовность защитных сооружений к приему нуждающихся в укрытии.

Защитные свойства укрытий от *ионизирующих излучений* рассчитывают по методикам, заложенным в специальных руководствах.

Оценка инженерной защиты завершается составлением плана мероприятий по обеспечению надежной защиты работников объекта и населения.

Оценивается устойчивость элементов объекта экономики к воздействию ударной волны, светового излучения, радиоактивного заражения, ЭМИ, отравляющих веществ и др.

Объекты экономики отличаются друг от друга как по характеру производства, так и по технологическому процессу и конструктивному решению. Поэтому оценка устойчивости элементов промышленного и сельскохозяйственного производства имеет некоторые особенности.

Оценка воздействия ударной волны ядерного взрыва. Критерием для определения устойчивости объектов экономики к воздействию ударной волны ядерного взрыва является величина избыточного давления, при которой элементы зданий, сооружений и инженерных коммуникаций либо сохраняются, либо получают слабые и частично средние разрушения.

Оценивать начинают с получения от штаба ГО ЧС района величины избыточного давления во фронте ударной волны, ожидаемой на объекте. При оценке устойчивости сооружений выявляются наиболее уязвимые элементы и участки, от которых зависит работа всего объекта. Результаты оценки устойчивости зданий, сооружений и коммуникаций к избыточному давлению обобщаются в виде таблицы.

Оценка устойчивости отдельных сооружений ложится в основу оценки объекта в целом. При этом его устойчивость определяют по тому зданию и сооружению, которое разрушается при наименьшем избыточном давлении.

В соответствии с оценкой устойчивости объекта разрабатывают мероприятия по повышению устойчивости наиболее уязвимых зданий или сооружений к воздействию ударной волны ядерного взрыва. При этом учитываются целесообразные пределы повышения устойчивости каждого здания и строения.

Оценка воздействия светового излучения. Устойчивость объекта к воздействию светового излучения оценивают по способности сооружения противостоять загоранию и возникновению пожаров по степени огнестойкости. Огнестойкость сооружений зависит, прежде всего, от качественных особенностей строительных материалов, использованных при возведении зданий.

Предел огнестойкости конструкций определяется временем в часах, в течение которого не появляются сквозные трещины и сооружение не теряет несущей способности, не обрушивается и не нагревается до температуры порядка 200°С на противоположной стороне.

По устойчивости к огню все строительные материалы делятся на несгораемые, трудносгораемые и сгораемые материалы.

Несгораемые – это такие материалы, которые под воздействием огня или высокой температуры не воспламеняются, не горят и не обугливают-

ся. К ним относятся все естественные и искусственные неорганические вещества, такие как кирпич, камень, бетон и др., а также применяемые в строительстве металлы.

Кирпичные, каменные и бетонные здания и сооружения относят к огнестойким, так как у них все части выполнены из несгораемых материалов.

Трудносгораемые – материалы, которые обладают свойством под воздействием огня или высокой температуры с трудом воспламеняться, не тлеют и не обугливаются или продолжают гореть или тлеть только при наличии источника огня. К ним относят асфальтовый бетон, гипсовые и бетонные детали с органическими наполнителями, глиносоломенные материалы, цементный фибролит, древесину, подвергнутую глубокой пропитке антипиренами, войлок, вымоченный в глинистом растворе, и др.

Сгораемые материалы под воздействием огня или высокой температуры воспламеняются или тлеют и продолжают гореть или тлеть после удаления источника огня. К ним относятся все органические вещества, не пропитанные антипиренами.

Самыми опасными являются помещения, здания и сооружения, возведенные из сгораемых материалов. Однако даже здания и сооружения, выполненные из сгораемых материалов, могут выдерживать воздействие огня или высоких температур какое-то, пусть и непродолжительное, время.

Особую опасность в противопожарном отношении представляют сооружения, возведенные из дерева.

При оценке устойчивости сооружений объекта вначале изучаются характер каждого строения и наиболее легковозгораемые элементы его, а также величина светового импульса, ожидаемого в районе объекта.

При оценке устойчивости объекта к световому излучению внимательно изучают все строения, расположенные в радиусе возможного возгорания, анализируется разрыв между ними, а также последствия, которые могут возникнуть от пожара, с учетом характера производства и плотности застройки. Возникновение единичных пожаров и превращение их в сплошные зоны огня определяются плотностью застройки.

Оценка воздействия радиоактивного заражения. Работа объекта в первую очередь будет зависеть от степени поражения ионизирующими излучениями его рабочих и служащих и заражения выпускаемой промышленностью продукции радиоактивными веществами. Критерием определения устойчивости является максимально допустимая доза облучения, которая не приводит к потере работоспособности и заболевания людей лучевой болезнью.

Оценка устойчивости объекта к воздействию этих факторов включает определение коэффициента ослабления радиации зданиями и сооружениями. По результатам оценки защитных свойств зданий и сооружений от ионизирующих излучений разрабатываются мероприятия по защите рабочих и служащих предприятия.

Оценка воздействия электромагнитного импульса. Критерием устойчивости к ЭМИ является наличие на объекте подавителей пиковых напряжений и нагрузок (ППНН), которые они могут выдержать по сравнению с максимально возможными нагрузками при ядерных взрывах. Подавители пиков напряжений включают в себя газонаполненные или вакуумные искровые разрядники, обеспечивающие уровень защиты от нескольких сотен до десятков тысяч вольт и быстродействие до нескольких наносекунд.

Оценка устойчивости системы управления, связи и оповещения. Управление объектом составляет основу деятельности руководства ГО ЧС по своевременному и успешному выполнению поставленных перед ним задач. Критериями устойчивости системы управления являются:

- Наличие и состояние оборудования противорадиационного укрытия (ПРУ).
- Надежность:
  - защиты личного состава и ПРУ и узлов (средств) связи;
  - функционирования системы связи и оповещения.
- Структура и возможности расчетов ПРУ.

В процессе оценки определяют:

- тип и емкость автоматизированных телефонных станций (АТС);
- мощность радиоузла;

♦ возможности диспетчерской связи;

♦ техническое состояние средств радио- и проводной связи, компьютерных комплексов;

♦ реальность и надежность схемы оповещения руководящего состава;

♦ места установки и техническое состояние средств подачи звуковых и световых сигналов (сирены, динамики);

♦ надежность защиты узла и линий связи от воздействия ударной волны, ЭМИ и радиоактивных излучений ядерного взрыва;

♦ возможность:

- взаимного дублирования проводной радиосвязью и наоборот,
- использования подвижных средств связи;

♦ наличие:

– резерва средств связи, материалов, запасных деталей и элементов для восстановления поврежденных участков линий связи,

– передвижных электростанций для зарядки аккумуляторов.

После завершения оценки разрабатываются мероприятия по повышению устойчивости системы управления, связи и оповещения.

8.2.3 Основные мероприятия по повышению устойчивости работы объектов экономики

Основные мероприятия по повышению устойчивости, проводимые на объектах в мирное время, предусматривают:

- Защиту рабочих и служащих и инженерно-технического комплекса:
  – от последствий стихийных бедствий, аварий (катастроф);
  – первичных и вторичных поражающих факторов ядерного взрыва.
- Обеспечение надежности управления и материально-технического снабжения.
- Светомаскировку объекта.
- Подготовку объекта к восстановлению нарушенного производства и переводу на режим работы в условиях ЧС.

Надежная защита рабочих и служащих от поражающих факторов является важнейшим условием повышения устойчивости работы любого объекта экономики. С этой целью возводятся защитные сооружения

типа убежищ для укрытия наибольшей части персонала работающей смены и пункта ПРУ в загородной зоне для неработающей смены и членов семей работников этого предприятия.

На участках с непрерывным производственным процессом строятся индивидуальные убежища с дистанционным управлением технологическими процессами.

Проводятся подготовительные мероприятия по рассредоточению и эвакуации в загородную зону производственного персонала и членов семей.

Выполняются мероприятия по накоплению, хранению и поддержанию готовности средств индивидуальной защиты.

Важнейшим элементом подготовки к защите является обучение рабочих и служащих умелому применению средств и способов защиты, действиям в ЧС, а также в составе формирований при проведении спасательных работ и оказанию первой доврачебной помощи.

Защита инженерно-технического комплекса предусматривает сохранение материальной основы производства: зданий и сооружений, технологического оборудования и коммунально-энергетических сетей.

Здания и сооружения при строительстве на объекте размещаются рассредоточенно. Между зданиями предусматриваются противопожарные разрывы шириной, суммарно равной высоте двух соседних зданий (не менее).

Наиболее важные производственные здания строят заглубленными или пониженной высоты, по конструкции – лучше железобетонные с металлическим каркасом. В каменных зданиях перекрытия должны быть из армированного бетона или из бетонных плит. Большие здания следует разделять на секции несгораемыми стенами (брандмауэрами).

Складские помещения для хранения ЛВЖ (бензина, керосина, нефти, мазута) размещаются в отдельных блоках заглубленного или полузаглубленного типа у границ объекта или за ее пределами.

От устойчивости зданий и сооружений зависит в основном устойчивость функционирования всего объекта. Поэтому повышение устойчивости зданий и сооружений достигается устройством каркасов, рам, подкосов, контрфорсов, промежуточных опор для уменьшения пролета несущих конструкций. Невысокие сооружения для повышения их прочности частично обсыпаются грунтом.

Высокие сооружения для повышения их прочности (трубы, вышки, башни, колонны) закрепляются оттяжками, рассчитанными на воздействие скоростного напора ударной волны.

Защита емкостей со СДЯВ и ЛВЖ осуществляется путем их обвалования (создания земляного вала вокруг емкости, рассчитанного на удержание полного объема жидкости).

Основные мероприятия по повышению устойчивости технологического оборудования ввиду его более высокой прочности по сравнению со зданиями, в которых оно размещается, заключаются в сооружении над ним специальных устройств в виде кожухов, шатров, зонтов и т. п., защищающих его от повреждения обломками разрушающихся конструкций. При недостаточной устойчивости самого оборудования в целях повышения сохранности после действия скоростного напора ударной волны оно должно быть прочно закреплено на фундаментах анкерными болтами.

При реконструкции и расширении промышленных объектов наиболее ценное и уникальное оборудование размещается на нижних этажах, в подвальных помещениях или в специальных защитных сооружениях. Целесообразно также размещать его в отдельно стоящих зданиях павильонного типа, имеющих облегченные и несгораемые ограждающие конструкции, разрушение которых не повлияет на сохранность оборудования.

Повышение устойчивости систем электроснабжения достигается проведением как общегородских, так и объектовых инженерно-технических мероприятий. Электроэнергия должна поступать на объект как минимум с двух направлений. При энергопитании с одного направления предусматривается автономный (аварийный) источник (передвижная электростанция).

Трансформаторные помещения, распределительная аппаратура и приборы надежно защищаются, в том числе и от электромагнитного импульса ядерного взрыва.

Особое внимание должно уделяться обеспечению *устойчивости систем снабжения газом.* Вся система подачи газа должна быть закольцована, что позволит отключить поврежденные участки и использовать

сохранившиеся линии. На газопроводах следует устанавливать запорную арматуру с дистанционным управлением и краны, автоматически перекрывающие подачу газа при разрушении труб.

Исключительное значение отводится созданию *устойчивой системы водоснабжения объекта.* Обеспечение водой должно осуществляться от двух источников – основного и резервного, один из которых должен быть подземным (артезианская скважина). Резервными источниками могут быть близко расположенный водоем, от которого к объекту заблаговременно подводится трубопровод, а также резервуары с запасом воды, защищенные от радиоактивного, химического и биологического заражения. Сети водоснабжения оборудуются задвижками для отключения отдельных участков при авариях.

Устойчивость работы объектов во многом определяется также *надежностью функционирования систем паро- и теплоснабжения.* Промышленные объекты должны всегда иметь два источника пара и тепла – внешний (ТЭЦ) и внутренний (местные котельные). Котельные размещаются в подвальных помещениях или специально оборудованных отдельно стоящих защитных сооружениях. Тепловая сеть закольцовывается, параллельные участки соединяются. Паропроводы прокладываются под землей в специальных траншеях. На паротепловых сетях устанавливаются запорные регулирующие приспособления.

Для повышения устойчивости канализации строятся раздельные системы: одна – для ливневых сточных вод, другая – для промышленных и хозяйственных (фекальных) сточных вод. В системе промышленной и хозяйственной канализации оборудуется не менее двух выпусков в городские коллекторы. На случай аварии в городских сетях и на насосных станциях система канализации должна иметь аварийные сбросы в расположенные вблизи карьеры, овраги или в ливневую сеть.

Дополнительно к перечисленным на объектах проводятся следующие мероприятия. Максимально сокращаются запасы взрывоопасных, горючих и сильнодействующих ядовитых веществ непосредственно на производственной территории, а сверхнормативные запасы вывозятся на безопасное расстояние, На трубопроводах устанавливаются автоматические отключающие устройства и клапаны – отсекатели, перекрывающие вышедшие из строя участки.

Для целей нейтрализации на химических предприятиях со СДЯВ необходимо иметь запас различных дегазационных веществ (щелочей, водного раствора аммиака, сернистого натрия и др.). В цехах оборудуется автоматическая сигнализация, которая позволит вовремя предупреждать об авариях, взрывах и загазованности территории. В случае необходимости предусматривается строительство защитных дамб для предупреждения возможности затопления территории, подготавливаются и рационально размещаются необходимые средства пожаротушения.

Для непрерывного управления на объекте при ЧС предусматривается наличие:

- надежно защищенных пунктов управления,
- диспетчерских пунктов,
- АТС и радиоузла,
- резервной электростанции для зарядки аккумуляторов АТС и питания радиоузла,
- систем надежной связи с местными органами, вышестоящим руководством ГО и штабом, с формированиями на объекте и в загородной зоне,
- эффективной системы оповещения должностных лиц и всего производственного персонала предприятия.

Надежность материально-технического снабжения обеспечивается организацией устойчивых производственных связей с предприятиями-поставщиками; заблаговременной подготовкой складов для хранения готовой продукции; переходом на местные источники сырья и топлива; строительством за пределами крупных городов филиалов предприятий; созданием на объектах запасов сырья, топлива, оборудования, материалов и комплектующих деталей; организацией перемещения запасов ресурсов в пределах объединения, отрасли.

Светомаскировка объектов экономики проводится для затруднения их обнаружения и опознания авиацией в темное время суток оптическими средствами. Она включает мероприятия по снижению освещенности населенных пунктов и объектов экономики, интенсивности сигнальных, транспортных и производственных огней, имитацию демаскирующих признаков на специально созданных ложных объектах.

Подготовка объектов к восстановлению предусматривается планами первоочередных восстановительных работ по нескольким вариантам возможного повреждения, разрушения объекта с использованием сил самих объектов, имеющихся строительных материалов, с учетом в случае необходимости размещения оборудования на открытых площадках, перераспределения рабочей силы, помещений и оборудования.

Для обеспечения сохранности технической документации рекомендуется изготовление копий в виде микрофильмов, гибких компьютерных дисков, один экземпляр которых должен храниться в загородной зоне.

Для своевременного и организованного проведения мероприятий по повышению устойчивости объекта разрабатывается план-график последовательности их осуществления в чрезвычайной ситуации.

ГЛОССАРИЙ

АДМИНИСТРАТОР ЗАЩИТЫ – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННАЯ – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы.

ВЕРИФИКАЦИЯ – процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

ВЛАДЕЛЕЦ СЕРТИФИКАТА КЛЮЧА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах.

ДИСКРЕТНОЕ УПРАВЛЕНИЕ ДОСТУПОМ – разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту

ДИСПЕТЧЕРЫ ДОСТУПА (ядро защиты) – технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

ДОКУМЕНТ – средство закрепления различным способом на специальном материале информации о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека.

ЗАКРЫТЫЙ КЛЮЧ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах элект-

ронной цифровой подписи с использованием средств электронной цифровой подписи.

ЗАЩИТА МНОГОУРОВНЕВАЯ – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

ЗАЩИТНОЕ СРЕДСТВО ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (защищенная автоматизированная система) – средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

ИДЕНТИФИКАТОР ДОСТУПА – уникальный признак субъекта или объекта доступа.

ИДЕНТИФИКАЦИЯ – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИНФОРМАЦИОННАЯ СИСТЕМА ОБЩЕГО ПОЛЬЗОВАНИЯ – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

КАНАЛ УТЕЧКИ ИНФОРМАЦИИ – совокупность источника информации, материального носителя или среды распространения несущего эту информацию сигнала и средства выделения информации из сигнала или носителя.

КЛАСС ЗАЩИЩЕННОСТИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ – определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ – информация, требующая защиты.

КОНЦЕПЦИЯ ДИСПЕТЧЕРА ДОСТУПА – концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.

КОРПОРАТИВНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА — информационная система, участниками которой может быть ограниченный круг лиц, оп-

ределенный ее владельцем или соглашением участников этой информационной системы.

МАНДАТНОЕ УПРАВЛЕНИЕ ДОСТУПОМ – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

МЕТКА КОНФИДЕНЦИАЛЬНОСТИ (МЕТКА) – элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

МНОГОУРОВНЕВАЯ ЗАЩИТА – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

МОДЕЛЬ ЗАЩИТЫ – абстрактное описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

МОДЕЛЬ НАРУШИТЕЛЯ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА – абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

НАРУШИТЕЛЬ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА – субъект доступа, осуществляющий несанкционированный доступ к информации.

НЕСАНКЦИОНИРОВАННЫЙ ДОПУСК – действия противника, приводящие к его ознакомлению с содержанием ценной информации или пользованию программными средствами без ведома их владельца.

НЕСЧАСТНЫЙ СЛУЧАЙ – случай с работающим, связанный с воздействием на него опасного производственного фактора.

ОКРЫТЫЙ КЛЮЧ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

ПАРОЛЬ – идентификатор субъекта доступа, который является его (субъекта) секретом.

ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ) – характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

ПОДТВЕРЖДЕНИЕ ПОДЛИННОСТИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ЭЛЕКТРОННОМ ДОКУМЕНТЕ – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

ПОЛЬЗОВАТЕЛЬ СЕРТИФИКАТА КЛЮЧА ЦИФРОВОЙ ПОДПИСИ – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

СЕРТИФИКАТ ЗАЩИТЫ (СЕРТИФИКАТ) – документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

СЕРТИФИКАТ КЛЮЧА ЦИФРОВОЙ ПОДПИСИ – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

СЕРТИФИКАТ СРЕДСТВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

СЕРТИФИКАЦИЯ УРОВНЯ ЗАЩИТЫ (СЕРТИФИКАЦИЯ) – процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

СЕРТИФИКАЦИЯ – это деятельность по подтверждению соответствия установленным требованиям независимой от изготовителя (продавца, исполнителя) и потребителя (покупателя) организации.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА – комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа информации в автоматизированных системах.

СИСТЕМА ЗАЩИТЫ СЕКРЕТНОЙ ИНФОРМАЦИИ – комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА – совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

СОБЫТИЕ НЕГАТИВНОЕ – это любое незапланированное событие, результатом которого выступает материальный ущерб или моральный урон предприятию, коммерческой или предпринимательской деятельности и влекущее за собой убытки, дополнительные расходы.

СРЕДСТВА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

СРЕДСТВО ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

УГРОЗА БЕЗОПАСНОСТИ ИНФОРМАЦИИ – действие, направленное против объекта защиты, проявляющееся в опасности искажений и потерь информации.

УСЛОВИЯ ТРУДА – совокупность факторов среды и трудового процесса.

УЩЕРБ (как термин) – фактические и возможные социальные и экономические потери и (или) ухудшение состояния (качества) экономической (коммерческой, предпринимательской) сферы деятельности.

УЩЕРБ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ – изменение информации, приводящее к нарушению ее вида или качества.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ – система правовых, организационных и других мероприятий и средств, направленная на защиту физического лица от внешней угрозы в любое время и в любом месте пространства на период обладания этим лицом конфиденциальной информации и определенными секретами коммерческой организации.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

ЭЛЕКТРОННЫЙ ДОКУМЕНТ – документ, в котором информация представлена в электронно-цифровой форме.

ЭЛЕКТРОННАЯ КОММЕРЦИЯ – заключение на международных и внутренних рынках в компьютерной форме различных сделок.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

СОДЕРЖАНИЕ

Учебное издание

Засканов Виктор Гаврилович
Несоленов Геннадий Фёдорович

БЕЗОПАСНОСТЬ В СФЕРЕ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

Часть II

Редактор Т.К. Кретинина
Компьютерная верстка И.И. Спиридонова

Подписано в печать 16.12.05. Формат 60x84 1/16.
Бумага офсетная. Печать офсетная.
Усл.печ.л. 11,0 . Усл.кр.-отт. 11,1 . Уч.-изд. л. 11,25 .
Тираж 200 экз. Заказ 33 .

Самарский государственный аэрокосмический университет.
443086 Самара, Московское шоссе, 34.

РИО Самарского государственного аэрокосмического университета.
443086 Самара, Московское шоссе, 34.